МАТЕРІАЛИ VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: «ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»

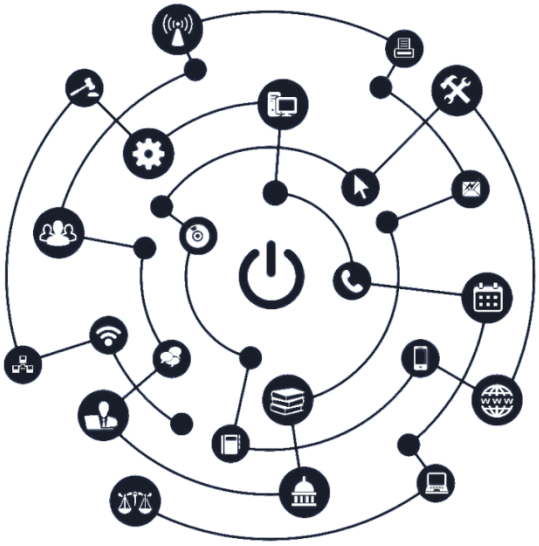
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ОДЕСА
20 травня 2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра інформаційних технологій



ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

20 травня 2022 року, м. Одеса

Одеса, 2022

УДК 340.12:316.3

ББК 67.0

Відповідальній редактор:
Н. І. Логінова, завідувач кафедри інформаційних технологій, к.пед.н., доцент

Друкується за рішенням кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
(протокол засідання кафедри № 11 від 09.05.2022 р.)

Матеріали VII Всеукраїнської науково-практичної конференції «Інформаційне суспільство: проблеми та перспективи» (м. Одеса, 20 травня 2022 р.). Одеса, 2022. 151 с.

Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи» присвячена розгляду актуальних питань розвитку інформаційного суспільства в Україні.
До участі у конференції запрошені студенти, аспіранти, молоді вчені, викладачі та науковці.
Конференція проводиться на базі Національного університету «Одеська юридична академія».

ПЕРЕДМОВА

Сучасні інформаційно-комунікаційні технології пронизують практично усі сфери діяльності людини: політику, економіку, бізнес, освіту, охорону здоров'я, державне управління, соціальну сферу, дозвілля тощо. Використання інформаційно-комунікаційних технологій дозволяє підвищити ефективність прийняття багатьох рішень за рахунок своєчасного отримання необхідної інформації.

Наразі спостерігаються бурхливі процеси розвитку інформаційних відносин, які є наслідком еволюції інформаційно-комунікаційних технологій. Ці процеси несуть як позитивний ефект, що відображається в забезпеченні прав громадян на інформацію та реалізації їх інформаційних потреб, так і потенційну небезпеку зловживання певною інформацією та заподіяння шкоди інформаційним правам та інтересам особи. За умов воєнного часу актуальними стають питання вибору достовірної інформації, попередження несанкціонованого та безконтрольного поширення інформації.

Технологічні та юридичні аспекти комп'ютерних злочинів, інформаційна та кібернетична безпека, особливості обробки даних за допомогою інформаційно-комунікаційних технологій в різних галузях знань, електронне врядування, захист інформації, інформаційні війни, право на інформацію, надійність та ефективність сучасних інформаційно-комунікаційних технологій, принципи формування та функціонування інформаційного середовища, управлінські та економічні аспекти розвитку сучасної IT індустрії – ось далеко неповний перелік питань, що цікавлять сьогодні молодіжне наукове середовище, і які склали основну тематику доповідей учасників конференції.

Ми сподіваємося на подальшу плідну роботу наукової молоді та цікавий обмін досвідом щодо розвитку сучасного інформаційного суспільства в Україні.

Секція 1. СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ЖИТТІ ЛЮДИНИ ТА СУСПІЛЬСТВА

АНАЛІЗ АКТИВНОСТІ КОРИСТУВАЧА ЗА ПРОФІЛЕМ ОПЕРАЦІЙНОЇ СИСТЕМИ iOS

Апанасенко А.С.

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У наш час інформаційні технології все міцніше входять у повсякденне життя, і комп'ютер став уже звичною її частиною. Для більшості людей, що мали досвід спілкування з комп'ютером, слова «іконка», «вікно», «робочий стіл», «меню Пуск» стали звичними й зрозумілим, а логотип чотириколірного прапорця, що розвівається, не викликає подиву.

У звичних нам мобільних комп'ютерних пристроях також є операційна система, яка допомагає нам більш зручніше й оперативніше управляти нашим мобільним пристроєм. Питання, пов'язані з кишеньковими комп'ютерами, смартфонами й комунікаторами, сьогодні стають актуальними, особливо у зв'язку з активним розвитком цього сегмента ринку й стрімким зростанням популярності різноманітних портативних пристроїв.

Будь-яка операційна система оперує деякими сутностями, які разом зі способами управління ними багато в чому характеризують її властивості. До таких сутностей можуть ставитися поняття процесу, об'єкта, файлу та ін. Кожна ОС має свій набір таких сутностей, і вже через управління цією сутністю надаються всі можливі функції. Однією з найпопулярнішою операційною системою в світі є iOS – мобільна операційна система для смартфонів, електронних планшетів, програвачів і деяких інших пристроїв, що розробляються і випускаються американською компанією Apple [1].

Мобільні операційні системи, такі як iOS, відрізняються від більшості інших операційних систем, оскільки вони поставляють кожен додаток у власну захисну оболонку, що заважає іншим застосункам порушувати їх. Це робить неможливим зараження вірусом застосунків у мобільній операційній системі, хоча існують і інші форми шкідливого програмного забезпечення. Захисна оболонка навколо застосунків також становить обмеження, оскільки вона не дозволяє безпосередньо спілкуватися між собою програмами. iOS оминула це, використовуючи розширюваність – функцію, яка дозволяє застосунку схвалювати для зв'язку з іншим застосунком.

Експерти стверджують, що мобільна платформа iOS набагато захищена операційна система перед більшістю видів існуючих атак. Пов'язано це в чималому ступені із суворим цензуруванням App Store.

В будь-якій роботі на першому місці завжди стоїть безпека, пише сайт Anonymous. Під безпекою мається на увазі захист від шкоди і інших небажаних наслідків. Всім потрібна безпека. Навіть смартфонам. Експертами з безпеки в мережі pCloud було проведено дослідження в ході якого було здійснено аналіз даних конфіденційності. З'ясувалося, які програми можуть передавати стороннім сервісам інформацію про користувача.

Є міф про те, що iOS забезпечує повну захищеність інформації, але це не зовсім так. Компанія Apple велику увагу приділяє захисту смартфона від шкідливих програм. Тому, не пропускає їх в App Store. Але, навіть не зважаючи на це найпростішим способом отримати особисті дані користувача є соціальна інженерія. Особливо добре вона спрацьовує на айфон, якщо користувач нехтує простими правилами [2]. Частою причиною є неуважність самого користувача. Але, існує й інша загроза крадіжки особистих даних, а саме з боку уряду, спецслужб і хакерів. Так, наприклад, останні можуть продавати інформацію внаслідок чого спецслужби можуть отримувати дані зі смартфона користувача. І навіть якщо це звучить досить нереально, насправді все так і відбувається навіть на iOS.

Слід брати до уваги, що не зважаючи, на заявлену безпеку системи iOS, існує загроза використання зібраних даних сторонніми особами. Починаючи, задля таргетованої реклами, закінчуючи кібершахраями. На наш погляд, доцільно використовувати Моніторинг активності користувачів – User Activity Monitoring (UAM). UAM фіксує дії користувача, у тому числі використання програм, відкриття вікон, виконання системних команд, натискання прапорців, введення/редагування тексту, відвідані URL-адреси та майже всі інші події на екрані для захисту даних, гарантуючи, що співробітники та підрядники залишаються в межах призначених їм завдань і не становить ризику для організації.

Програмне забезпечення для моніторингу активності користувачів може відтворювати дії користувача як відео та обробляти відео в журналах активності користувачів, які ведуть покрокові записи дій користувача, які можна шукати та аналізувати для розслідування будь-яких невідповідностей.

Список використаних джерел:

1. Compare iPhone models/ iPhone - Apple Official Sitehttps URL: //www.apple.com/
2. Apple Introduces New iPod touch. Apple Press Release URL: https://www.apple.com/newsroom/2010/09/01Apple-Introduces-New-iPod-touch/

Науковий керівник: Виходець О.О.

КОРЕЛЯЦІЙНИЙ ІМУНІТЕТ 4-ФУНКЦІЙ, ЩО СИНТЕЗОВАНІ НА ОСНОВІ КОРЕЛЯЦІЙНО-ІМУННИХ БУЛЕВИХ ФУНКЦІЙ

Бакуніна О. В.

кандидат фізико-математичних наук, доцент, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Розвиток сучасних методів криптографії багато в чому пов'язаний із використанням функцій багатозначної логіки (ФБЛ), які, разом з булевими функціями, дозволяють визначити рівень реалізації концепцій дифузії та конфузії сучасних криптографічних алгоритмів [1].

В даний час відомі набори критеріїв криптографічної якості як булевих функцій [2], так і функцій багатозначної логіки [3], серед яких найважливішими є критерії нелінійності (алгебраїчна та дистанційна нелінійність), критерії лавинного ефекту (критерій поширення помилки, суворий лавинний критерій, критерій максимального лавинного ефекту) та кореляційні критерії (критерій незалежності виходу від вхідних змінних, критерій кореляційного імунітету). Проте питання взаємозв'язку між критеріями криптографічної якості ФБЛ та їх компонентних булевих функцій залишаються недослідженими. Зокрема, у відкритих джерелах не представлена інформація про кореляційний імунітет 4-функцій, які синтезовані з кореляційно-імунних булевих функцій, незважаючи на те, що подібна операція була застосована в роботі [4] для синтезу S-блоків, кореляційно імунних як в сенсі компонентних булевих функцій, так і в сенсі компонентних 4-функцій.

Метою цієї роботи є встановлення взаємозв'язку між кореляційними властивостями 4-функцій довжини $N=16$, які синтезовані на основі кореляційно-імунних булевих функцій.

Введемо необхідні нам визначення кореляційного імунітету спочатку для булевих функцій.

Визначення 1 [2]. Булева функція $f(x)$, $x\in V_k$, називається кореляційно-імунною порядку m, $1\le m\le k$, якщо вихід $y=f(x_1^k)$ і будь-яка множина з m її вхідних змінних є статистично незалежними.

Визначення 2 [2]. Підфункцією булевої функції $f(x)$, $x\in V_k$ називається функція f', що отримана підстановкою в функцію f констант "0" або "1" замість частини змінних. Якщо підставимо в функцію f константи $\sigma_{i_1},\cdots,\sigma_{i_s}$ замість змінних $x_{i_1},\cdots,x_{i_s}$, відповідно, то отримана підфункція позначається $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$. Якщо

замість змінної x_i константа не підставлена, то x_i називається вільною змінною.

Наприклад, нехай задана булева функція $f(x_1, x_2, x_3)$, тоді її підфункціями є $f'(x_1, x_2, 0)$, $f'(x_1, x_2, 1)$, $f'(x_1, 0, 0)$, $f'(x_1, 0, 1)$ і т.д.

Визначення 3 [2]. Булева функція $f(x)$, $x \in V_k$, називається кореляційно-імунною порядку m, $1 \le m \le k$, якщо вага Гемінга дорівнює $wt(f') = wt(f)/2^m$, для будь-якої її підфункції f' від $k-m$ змінних.

У роботі [3] також були введені визначення кореляційного імунітету ФБЛ, основні з яких наведемо далі.

Для заданої послідовності f ми можемо ввести вектор $K = \{K_0, K_1, ..., K_{q-1}\}$, де K_u — кількість входжень символу $u \in \{0,1,...,q-1\}$ в послідовність f.

Визначення 4 [3]. Розбалансом послідовності f назвемо значення модуля суми поелементних добутків елементів вектора K на відповідні елементи експоненціального алфавіту $\{z_0, z_1, ..., z_{q-1}\}$

$$\Delta(f) = \left| K_0 z_0 + K_1 z_1 + ... + K_{q-1} z_{q-1} \right|. \quad (1)$$

На основі *Визначення 4* розбаланса ФБЛ вводиться визначення незалежності виходу 4-функцій від її вхідних змінних, а також визначення кореляційного імунітету 4-функцій.

Визначення 5 [3]. Підфункцією q-функції $f(x)$ називається функція f', отримана підстановкою у функцію f значень з множини $\{0,1,...,q-1\}$ замість деяких змінних. Якщо підставити у функцію f константи $\sigma_{i_1}, \cdots, \sigma_{i_s}$ замість змінних $x_{i_1}, \cdots, x_{i_s}$, відповідно, то отримана підфункція позначається $f^{\sigma_{i_1}, \cdots, \sigma_{i_s}}_{x_{i_1}, \cdots, x_{i_s}}$.

Визначення 6 [3]. Кажуть, що вихід 4-функції $f(x)$ є незалежним від групи своїх вхідних змінних $\{x_i\}$, $i = 1,...,m$ якщо при підстановці замість цих змінних будь-яких констант $\sigma_{i_1}, \cdots, \sigma_{i_s} \in \{0,1,2,3\}$, розбаланс отриманих таким чином підфункцій становить $\Delta_{f'} = \dfrac{\Delta_f}{4^m}$.

Визначення 7 [3]. Кажуть, що 4-функція $f(x)$ є кореляційно імунною порядку $m \le k$, якщо її вихід є незалежним щодо будь-якої групи з m своїх вхідних змінних,

тобто розбаланс її підфункцій $k-m$ змінних становить $\Delta_{f'} = \frac{\Delta_f}{4^m}$.

Для вирішення поставленого завдання було розроблено наступний алгоритм:

Крок 1. Пошук множини кореляційно імунних булевих функцій довжини $N=16$, кількість яких склала $J_2 = 222$, що збігається з результатом, отриманим у роботі [5].

Крок 2. Знаходження суперпозиції кожної можливої пари (враховуючи перестановки), отриманих на Кроці 1 булевих функцій, як це показано в прикладі

$$\begin{array}{rcccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ f_{20} = & \{ & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \} \\ f_{21} = & \{ & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \} \\ f_{4} = & \{ & 0 & 0 & 0 & 2 & 1 & 3 & 3 & 3 & 3 & 3 & 1 & 2 & 0 & 0 & 0 & 0 & \}. \end{array} \quad (2)$$

На даному етапі ми отримуємо $J_4 = 222^2 = 49284$ 4-функції.

Крок 3. Дослідження кореляційних властивостей отриманих на Кроці 2 4-функцій відповідно до умов Визначення 6 та Визначення 7.

Виконуючи дослідження відповідно до представленого алгоритму ми отримали результати, які для зручності представимо в табл. 1.

Таблиця 1. Результати дослідження множини 4-функцій, отриманої на основі суперпозиції кореляційно-імунних булевих функцій

Кореляційні властивості	Потужність множини	% від усіх отриманих 4-функцій
4-функції, вихід яких не залежить від змінної x_1	6 308	12.8%
4-функції, вихід яких не залежить від змінної x_2	6 308	12.8%
Кореляційно-імунні 4-функції	1 028	2.09%
4-функції загального виду	35 640	72.31%
Всього	49 284	100%

Результати аналізу даних, представлених у табл. 1 приводять до висновку, що отримання кореляційно-імунної 4-функції на основі двох кореляційно-імунних булевих функцій відбувається тільки в 2.09% випадків, що свідчить про істотні відмінності в природі кореляційного імунітету булевих функцій і ФБЛ і підтверджує необхідність дослідження сучасних криптографічних алгоритмів при їх поданні як за допомогою математичного апарату булевих функцій, так і за допомогою

математичного апарату ФБЛ.

Відзначимо основні результати проведених досліджень:

1. Розроблено алгоритм вивчення кореляційних властивостей 4-функцій, синтезованих на основі кореляційно-імунних булевих функцій.

2. Визначено кількості 4-функцій, вихід яких не залежить від змінних x_1 або x_2, а також кореляційно-імунних 4-функцій, які можуть бути синтезовані на основі кореляційно-імунних булевих функцій.

3. Отримані результати характеризують рівень взаємозв'язку між кореляційним імунітетом булевих функцій і ФБЛ, які побудовані на їх основі, що є важливим для визначення кореляційних властивостей сучасних криптоалгоритмів.

Список використаних джерел:

1. Shannon C. E. A Mathematical Theory of Cryptography. USA : Bell System Technical Memo, 1945, MM 45-110-02.
2. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.
3. Соколов А. В., Жданов О. Н. Криптографические конструкции на основе функций многозначной логики. Монография. М: Научная мысль, 2020. 192 с.
4. Бакунина Е. В. О существовании класса s-блоков, удовлетворяющих корреляционному иммунитету компонентных булевых функций и 4-функций. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру*: у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 603-606.
5. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89. Київ: *Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія»*. 2009. С. 5-12.

ЗНАЧЕННЯ ТА ВПЛИВ МАТЕМАТИЧНОЇ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІТ-ТЕХНОЛОГІЙ

Баландіна Н. М.

старший викладач кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Галузь ІТ-технологій вже змінила світ та продовжує відігравати ключову роль в його подальшому розвитку. Тому професійні кадри в галузі інформаційних технологій є одними з найбільш затребуваних на ринку праці розвинутих країн. Але нині мова йде про підготовку такого фахівця, який вміє в потрібний момент знайти необхідну інформацію, проаналізувати її, зіставити одержану інформацію

із задачами, які необхідно розв'язати, та на цій основі виробити адекватні шляхи розв'язання поставленої задачі [1].

Професійна діяльність ІТ-фахівців нині багатоаспектна та вимагає глибоких знань у відповідних галузях застосувань, проте ці знання не дадуть очікуваного результату без фундаментальної математичної підготовки. У зв'язку з чим зростає роль математичної складової професійної компетентності сучасних ІТ-фахівців [2].

Відомо, що кожна спеціальність має свій мінімальний набір обов'язкових знань. У процесі підготовки фахівців у галузі інформаційних технологій такою основою служить математика. Професійний рівень майбутніх фахівців, їх конкурентоздатність та компетентність безпосередньо залежить від якості математичної освіти.

Математика є базою ефективного розв'язування завдань програмування, адміністрування баз даних, захисту і передачі інформації, розпізнавання образів, розробки програмного забезпечення тощо.

Сучасна математична освіта має за мету формування у майбутніх фахівців ІТ-напрямків математичної та інформаційної культури, розвиток логічного та абстрактного мислення, інтелектуальної підготовки до вирішення практичних задач, пов'язаних з професійною діяльністю.

Практика показує, що вимоги до рівня математичної підготовки програмістів з часом все більше зростають. І нині без ґрунтовної математичної підготовки підготувати висококваліфікованого програміста неможливо [1].

Математична освіта студента факультету кібербезпеки та інформаційних технологій починається на першому курсі навчання з вивчення дисциплін лінійної алгебри, аналітичної геометрії та математичного аналізу. Ці математичні дисципліни мають ряд точок дотику та перетини, складаючи фундамент сучасної математичної науки.

Вища математика для більшості першокурсників є дисципліною, під час освоєння якої, студенти нерідко стикаються з труднощами. Одна з причин цього – великий обсяг матеріалу, який потрібно освоїти за короткий час. Серед факторів, які негативно впливають на якість підготовки студентів можна вказати суттєве посилення ролі самостійної роботи при недостатньому розвитку у студентів навичок до самонавчання та саморозвитку.

У результаті отриманих в процесі навчання математичних знань у майбутнього фахівця з'являється математична культура, яка дозволяє йому оволодіти сучасним математичним апаратом, необхідним для вирішення практичних завдань, підготуватись до спеціальних дисциплін на старших курсах, розбиратися в

математичних методах дослідження та вироблення вміння самостійно розширювати свої знання з математики.

Особливо гостро проблема математичної підготовки постає для ІТ–фахівців, оскільки основу програмування складає не тільки знання певної мови програмування, а й уміння побудувати математичну модель, знання ефективних алгоритмів, процесу створення алгоритмів для розв'язання поставленого завдання [3].

Отже, якісна математична освіта є ключовою складовою у професійній підготовці майбутніх фахівців з ІТ-технологій.

Список використаних джерел:

1. Кучерук О.Я. Роль математичної підготовки у професійній підготовці ІТ–фахівців [PDF] с сайта khnu.km.ua_Роль математичної підготовки у професійній підготовці ІТ–фахівців
2. Кучерук О.Я. Математична підготовка як важлива складова професійної компетентності інженера-програміста *Materiały XI Międzynarodowej naukowi-praktycznej konferencji «Naukowa myśl informacyjnej powieki - 2015*» Volume 7. Pedagogiczne nauki.C.26–28
3. Щедролосьєв Д.Є. Дискретна математика як фундаментальна дисципліна в системі математичної підготовки майбутніх інженерів-програмістів / Д.Є. Щедролосьєв // *Інформаційні технології в освіті*, 2010. №5. С. 129–133. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/ itvo/2010_5/17.pdf.

ІНФОРМАЦІЙНА КУЛЬТУРА В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Дехніч А.В.

студент 1-го курсу судово-адміністративного факультету Національного університету «Одеська юридична академія»

Сьогоднішній етап розвитку цивілізації характеризується становленням глобального інформаційного суспільства, в якому основним ресурсом є інформація. Нові інформаційно-комунікаційні технології все більш широко проникають практично у всі сфери життєдіяльності суспільства, змінюючи умови праці і побуту людини, формуючи у нього нові потреби, стереотипи поведінки, а також нові уявлення про якість життя, простір і час.

У сучасному інформаційному суспільстві право громадянина на інформацію постає основоположним правом людини. Однак інформація не може мати змістовний сенс упродовж тривалого часу, тобто наповнюватися певним змістом без здійснення ефективної владно-громадської комунікації, тому комунікація влади та суспільства – це безперервний і фактично нескінченний процес.

Також слід зважати, що ефективність владно-громадського діалогу залежить від комунікаційних факторів, які формують рівень довіри до владних

інститутів і, відповідно, загальне ставлення до влади в суспільстві. Тобто дієвість діалогу влади та громади безпосередньо залежить від можливості громадян постійно перевіряти аспекти діяльності влади, звертаючись до різних джерел. Одним з основних чинників цього процесу є вільний доступ особи до інформації.

Аналіз сучасної державної комунікаційної політики засвідчує наявність низки проблем, розв'язання яких потребує ретельного опрацювання юридичного інструментарію підготовки управлінських рішень. Очевидним є те, що сучасна модель владно-громадських відносин не відповідає етапу розвитку України, насамперед – активній фазі становлення, формування та розвитку інформаційного суспільства.

Як вітчизняні, так і європейські науковці в перші роки XXI ст. констатують суттєві зміни геополітичної ситуації на європейському континенті, що насамперед пов'язані з глобальним зростанням обсягів інформації, які, зруйнувавши географічні кордони держав, стали каталізатором усесвітнього об'єднавчого процесу.

Новітні інформаційні технології частково послабили домінантну роль традиційних засобів масової комунікації як посередника в комунікаційній взаємодії органів державної влади та громади, проте останні залишаються важливим інструментом, за допомогою якого держава здійснює діалог із суспільством. У праці «Реальність мас-медіа» Н. Луман передбачав, що згодом поняттям «масмедіа мають бути охоплені всі публічні установи, які використовують технічні засоби для розповсюдження повідомлень.

Тож завдання, що нині постали перед українськими органами державної влади у сфері регулювання інформаційно-правових відносин, мають бути синхронізовані з тими, які постають у процесі формування принципових підходів до практичного створення умов розвитку інформаційного суспільства. Водночас потребують адаптації до світових принципів здійснення інформаційної політики положення вітчизняного законодавства публічної галузі (з обов'язковим збереженням національної ідентичності), а також визначення статусу суспільно важливої інформації в переліку видів інформації під час налагодження ефективної комунікації між органами державної влади та громадою.

Зокрема, у ст. 19 Загальної декларації прав людини (прийнята на третій сесії Генеральної Асамблеї ООН 10 грудня 1948 року) визначено, що кожна людина має право на свободу переконань і вільне вираження їх. Це право охоплює свободу безперешкодно дотримуватися своїх переконань і свободу шукати, одержувати й поширювати інформацію та ідеї будь-якими засобами незалежно від державних кордонів.

Після ратифікації Верховною Радою України 11 вересня 1997 року набула чинності Конвенція про захист прав людини і основоположних свобод, у ст. 10 «Свобода вираження поглядів» якою передбачено:

1. Кожен має право на свободу вираження поглядів, що охоплює свободу дотримуватися своїх поглядів, одержувати й передавати інформацію та ідеї без

втручання органів державної влади й незалежно від кордонів. Водночас стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

2. Здійснення публічних свобод, оскільки воно пов'язане з обов'язками та відповідальністю, може підлягати таким умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, захисту репутації чи прав інших осіб, запобігання розголошенню конфіденційної інформації або підтримання авторитету й безсторонності суду (Slinko, 2018).

Зокрема, П. Монк та Е. Монроу обстоюють думку, що питання демократизації процесу залучення громади до державного управління та формування підґрунтя інформаційного суспільства безпосередньо залежить від спроможності громади мати вільний доступ до публічної інформації, створеної в процесі діяльності органів державної влади, і гарантування прав на її збирання, зберігання й поширення.

Украй важливим є положення про те, що ст. 3 Закону України «Про інформацію» гарантує відкритий доступ кожної особи до інформації, і цей норматив постає одним із головних напрямів державної інформаційної політики. До основних складових державної інформаційної політики також належать: забезпечення однакових можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень тощо.

З огляду на важливий позитивний аспект прийняття Закону України «Про внесення змін до Закону України «Про інформацію» та Закону України «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних» як нормативних регуляторів інформаційно-правових відносин у державі, слід констатувати, що, водночас, виникла низка суперечок стосовно тлумачення понятійного апарату та юридичних наслідків регулювання порядку здійснення й забезпечення права кожного на доступ до інформації.

Невідповідність у термінах і дефініціях спричинена, передусім, сутністю поняття «інформація», яку в нормативно-правових документах України трактують по-різному. Наприклад, у Законі України «Про інформацію» зазначено, що «інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді». З позиції регулювання інформаційно-правових відносин суспільний інтерес можуть викликати не лише відомості й дані, які вже збережено на матеріальних носіях. Крім того, у Законі немає детального розподілу інформації за видами, що також ускладнює доступ до інформації, зокрема інформаційних даних, які можуть бути службовою або секретною інформацією.

У Законі України «Про доступ до публічної інформації» від 13 січня 2011 року вперше знаходимо нормативне тлумачення юридичного терміна «публічна інформація», що є «відображеною та задокументованою будь-якими засобами та на будь-яких носіях інформацією, яка була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом і частковою деталізацію видів інформації».

Цей законодавчий акт також не зміг ліквідувати наявні розбіжності й дефініції вітчизняної інформаційної сфери. Під час нормативно-правової ідентифікації понять «суб'єкти владних повноважень» ми констатуємо певні неузгодженості.

Наприклад, у Законі України «Про інформацію» «суб'єкт владних повноважень – це орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, зокрема на виконання делегованих повноважень». У Законі України «Про доступ до публічної інформації» – це вже більш розширений перелік органів та установ, а саме: «суб'єкти владних повноважень – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади

Отже, сучасне вітчизняне законодавство трактує ці види інформації так, що навіть своїми назвами вони об'єднують, взаємодоповнюють і, водночас, суперечать одна одній.

Затребуваність у започаткуванні ефективного та відкритого владно-громадського діалогу, незалежне формування громадянської позиції та впровадження стандартів інформаційного суспільства стримують застарілі догми щодо максимального втаємничення інформації, яка не репрезентує владу. Сучасні технології маніпулювання громадською думкою ресурсами державної інформаційної політики, які мають численні підтвердження в українській дійсності, не сприяють зміцненню довіри до влади, а отже, її легітимізації у свідомості громади, що може призвести до відкритих протистоянь влади й суспільства, які вже були в новітній вітчизняній історії.

Список використаних джерел:

1. Дзьобань О. П. Філософія інформаційного права: світоглядні й загальнотеоретичні засади : монографія / О. П. Дзьобань. Х. : Майдан, 2013. 360 с.
2. Андреев Д. В.. Транзактність соціально-правових комунікацій. URL: http://npnuola.onua.edu.ua/index.php/ 1234/ article/view/336/335.
3. Закон України «Про доступ до публічної інформації URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.
4. Конвенція про захист прав людини і основоположних свобод. URL: ст. 19 Загальної декларації прав людини. URL: https://bit.ly/3PmueeF.
5. ст. 10 «Свобода вираження поглядів». URL: https://bit.ly/39VvF3e.

Науковий керівник: доцент Задерейко О.В.

ОСОБЛИВОСТІ МЕТОДИКИ ВИКЛАДАННЯ ЗАНЯТЬ З ДИСЦИПЛІНИ «ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ»

Дика А.І.

асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Зараз підготовка фахівців носить традиційний лекційно-практичний характер. Безперечно, що такі форми навчання як «лекція» та «практичні заняття» є дієвими та доцільними. У процесі лекції здійснюється постановка проблемних питань, які краще використовувати у процесі вивчення теоретичного матеріалу.

Традиційно заняття дисципліни «Охорона праці та безпека життєдіяльності» (далі – охорона праці) зводяться до розгляду нормативно-правових документів і вивчення прийомів безпечного проведення робіт для підприємства. Однак це не сприяє підвищенню зацікавленості студентів у вивченні матеріалу.

Застосування сучасних технологій викладання дисципліни з охорони праці дозволяє видозмінити весь процес навчання, дає можливість викладачеві вносити до навчального процесу нові різноманітні форми та методи, що робить заняття цікавішим та є ефективним інструментом формування професійних компетенцій.

Зупинимося на основних інноваційних педагогічних технологіях, які можуть успішно використовуватись у викладанні курсу з основ охорони праці і безпеки життєдіяльності – це комп'ютерні технології, проєктний метод навчання, кейс метод, дидактичні ігри, інтерактивні методи навчання, диспути, круглі столи [1]. Розглянемо декілька технологій, які найчастіше використовуємо під час проведення практичних занять з основ охорони праці та безпеки життєдіяльності.

Комп'ютерні технології навчання. Ціль технології – формування умінь працювати з інформацією, розвиток комунікативних здібностей. Це можливо за наявності комп'ютеризації навчального закладу, сучасних форм надання інформації, вільного доступу до неї та особистих знань викладача. Все це уможливлює процес дистанційної передачі інформації. Навіть часткова комп'ютеризація дисципліни з основ охорони праці сприяє інтенсифікації навчання та поглибленню знань з дисципліни. Це і застосування електронних підручників, посібників, довідників, що підвищують рівень самоосвіти здобувачів. Також досить ефективним є застосування різних відео та аудіо записів з відповідної тематики дисципліни.

Використовувані на етапі пояснення нового навчального матеріалу інформаційні технології підвищують мотивацію до навчання, розвивають пізнавальні здібності студентів. Для коригування та контролю процесу навчання доцільно застосовувати тестові програмні засоби, які дозволяють автоматизувати процес та скоротити час контролю знань студентів.

Зміст інформації у галузі охорони праці досить великий і постійно змінюється, а застосування комп'ютерів на заняттях значно підвищує мотивацію до

навчання, підвищує інтерес у студентів до отримання нових знань, краще засвоюється і збільшується обсяг вивченої інформації в галузі охорони праці.

Вказане вирішує завдання з підвищення якості процесу навчання та засвоєння матеріалу, формування інформаційної культури. Використання комп'ютерних технологій дає змогу проводити навчання шляхом складення різноманітних тестів, логічних ланцюжків, тренувальних вправ, діаграм, графіки, виконання практичної роботи і працювати з Інтернет-ресурсами тощо [2]. У студентів закладаються основи естетики за допомогою використання комп'ютерної графіки, мультимедійних технологій. Формується методична скарбничка презентацій з різних розділів курсу безпеки життєдіяльності, які можна використовувати надалі на заняттях.

Застосування мультимедійних презентацій робить навчальний матеріал більш доступним, наочним і підвищує інтерес до дисципліни, що вивчається. Для вирішення такого завдання програма MS PowerPoint або Google Презентації надає викладачеві багато можливостей, тому що в них можливе використання текстової, графічної, звукової та відеоінформації. Мультимедійна презентація, створена в цих програмах, може стати універсальним дидактичним засобом, який дає можливість підвищення ефективності навчального процесу. Використання презентацій дозволяє зробити заняття більш щільним та насиченим за змістом.

В результаті досягаються ідеальні варіанти індивідуального навчання з використанням візуальних та слухових образів, створюється можливість залучення наукової та культурної інформації з різних джерел. Інформаційні технології вносять до освітнього процесу елементи новизни, наочності, що підвищує інтерес студентів до придбання знань, полегшує викладачеві підготовку до навчально-виховного процесу.

Проєктний спосіб навчання. Мета технології – розвиток пізнавальних, творчих навичок студентів, умінь самостійно конструювати свої знання, орієнтуватися в інформаційному просторі; розвиток критичного мислення.

На етапах створення проєкту діяльність викладача полягає у наступному: з носія готової інформації викладач перетворюється в організатора пізнавальної, дослідницької діяльності своїх студентів. Викладач допомагає студентам у пошуку джерел інформації, іноді сам надає інформацію на цю тему, підтримуючи безперервний зворотній зв'язок. На підготовчому етапі необхідно виділити ціль та завдання проєкту, вибрати потрібні методики роботи. На основному етапі складання проєкту викладач є координатором самостійної роботи студентів. На заключному етапі він робить акцент на підготовці студентів до публічного представлення проєкту.

Кейс-метод. На заняттях з дисципліни охорона праці розглядаються різні варіанти екстремальних ситуацій у мирний та воєнний час, їх наслідки для людей та навколишнього середовища, а також алгоритми дій в умовах небезпечних (надзвичайних) ситуацій та допомоги постраждалим у різних випадках внаслідок

виникнення цих екстремальних ситуацій. Враховуючи тематику матеріалу, що вивчається, а також необхідність використання інноваційних методів навчання, одним з найбільш відповідних інструментів формування компетенцій є кейс-метод. Суть технології полягає в тому, що в основі зазначеного методу використовуються описи конкретних ситуацій (випадків).

Студентам пропонується осмислити реальну життєву ситуацію, опис якої одночасно відображає не лише практичну проблему, алгоритм дій, а й актуалізує певний комплекс знань, який необхідно засвоїти при вирішенні цієї проблеми. До того ж сама проблема не має однозначного рішення. Слід зазначити, що роль викладача полягає у направленні бесіди або дискусії, наприклад, за допомогою додаткових питань; у контролі часу роботи; у спонуканні студентів відмовитися від поверхневого мислення; залученні всіх студентів групи до процесу аналізу [3].

Внаслідок застосування кейс-методу на практичних заняттях у студентів формуються вміння: аналізувати та встановлювати проблему; чітко формулювати, висловлювати та аргументувати свою позицію; спілкуватися, дискутувати, сприймати та оцінювати вербальну та невербальну інформацію; приймати рішення з урахуванням конкретних умов та наявності фактичної інформації.

Застосування сучасних технологій викладання на заняттях з «Охорони праці та безпека життєдіяльності» дозволить підвищити ефективність навчального процесу, рівень поінформованості та підготовки студентів, індивідуалізувати навчання, дозволить залучити студентів до навчального процесу, підвищити результативність навчання.

Список використаних джерел:

1. Шевченко Л. С. Застосування інноваційних педагогічних методик майбутніми учителями технологій. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми*: зб. наук. пр. Київ-Вінниця. 2015. вип. 43. С. 94-99.
2. Матвійчук Л.Ю. Застосування інформаційних технологій у процесі вивчення дисципліни «Безпека життєдіяльності». *Наукові записки Тернопільського національного педагогічного університету.* Серія: педагогіка. 2009. №3. С. 190.
3. Бужанська М. Особливості використання кейс-методу під час вивчення дисципліни «безпека життєдіяльності та охорона праці». *Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка*. Серія: педагогіка. 1, 1. 2021. С. 67-74.

ПІДГОТОВКА ТА АНАЛІЗ ДАНИХ ЗАСОБАМИ МОВИ ПРОГРАМУВАННЯ PYTHON

Дрига А.В.

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В наш час, коли технології все швидше заповнюють наше середовище, а великі масиви даних стали невід'ємною частиною життя, як ніколи важливо не тільки отримувати корисні знання з усього потоку інформації, але й уміти їх аналізувати та отримувати правильні висновки. Для цих цілей використовують методи візуалізації даних – дослідження інформації та її властивостей за допомогою візуальної презентації. Саме візуальна презентація допомагає людині знайти закономірність та значущість навіть у великому наборі даних.

Важливість візуалізації великих даних особливо себе показала під час виникнення пандемії COVID-19. З першого її дня кожен день надходила колосальна кількість інформації щодо захворюваності зі всіх куточків Землі, яку потрібно було аналізувати та на основі цього приймати рішення. Наприклад, перед багатьма країнами постало питання впровадження локдауну, а саме при якій кількості хворих потрібно йти на такий шаг та як це вплине на добробут населення, чи не призведе це до стрімкого росту безробіття. Тільки проаналізувавши політику двох країн щодо впровадження карантину та взявши відомості про темп розповсюдження коронавірусу та рівень безробіття в них можна сказати, чи варто впроваджувати жорсткий локдаун. А так як кількість даних про це величезна, для прорахунку кроків потрібно задіяти їх візуалізацію.

Перед тим, як приступити до візуальної презентації даних, потрібно обрати інструмент, за допомогою якого це буде якомога зручніше зробити. Було обрано об'єктно-орієнтовану мову програмування Python. Вона використовується для роботи з великим обсягом інформація в таких сферах, як генетика чи економічному аналізі через те, що має порівняно легкий синтаксис, що допомагає швидко писати програми, а також багато спеціалізованих бібліотек, наприклад Matplotlib або Plotly.

Розібравшись з інструментами, потрібно виконати такі завдання:

- обрати країни, що схожі за економічними та екологічними умовами, але які мали різну політику впровадження локдауну;
- знайти джерела інформації о захворюваності та безробітті в них;
- на основі джерел виконати візуалізацію даних;
- зробити висновок.

Для проведення аналізу було обрано Швецію та Норвегію через те, що вони максимально підходять за критеріями: обидві країни скандинавські та обидві мають симетрично різні підходи до вирішення питання з рівнем захворюваності населення на COVID-19. В той час, коли Швеція не задіяла ніяких карантинних

обмежень, Норвегія запровадила низку суворих правил задля зупинки розповсюдження коронавірусу.

Інформацію про безробіття та захворюваність обох країн було завантажено з офіційних джерел статистичної організації Європейської Комісії (Євростату) [1] та некомерційного видання Our World in Data [2] відповідно. Ці відомості можна використовувати безкоштовно, але вони представлені у двох різних форматах – TSV для даних о безробітті та JSON для даних о захворюваності. Python вміє без проблем працювати з файлами типу TSV, а для JSON файлів навіть існує спеціальна бібліотека json, яка допоможе видобувати та опрацювати інформацію.

Коли дані видобуто та збережено, можна їх візуалізувати. Це буде зроблено за допомогою вже зазначених бібліотек Matplotlib та Plotly. Отримаємо такий результат:

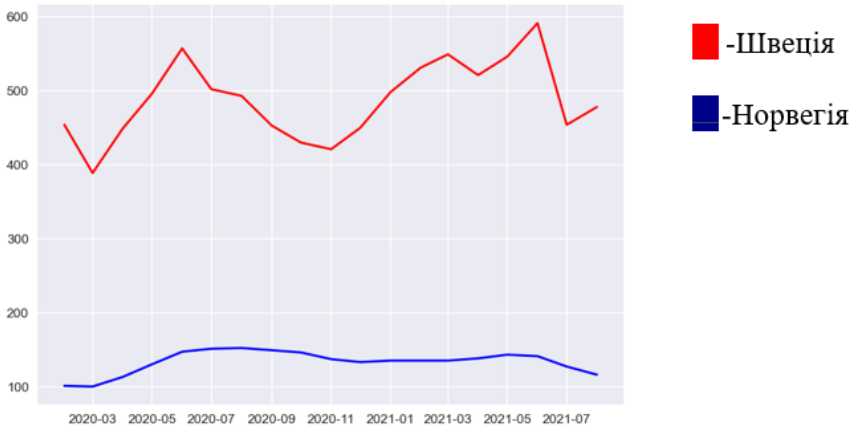


Рис. 1. Діаграми рівня безробіття в Норвегії та Швеції

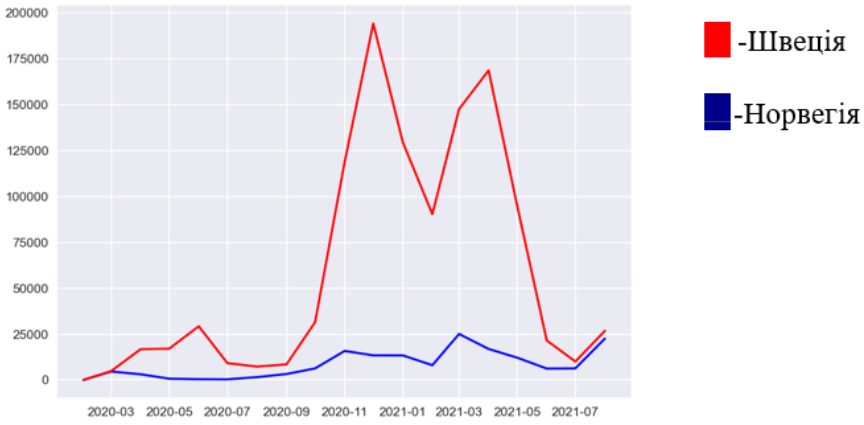


Рис. 2. Діаграми рівня захворюваності в Норвегії та Швеції

Як можна побачити, в обох випадках Швеція програє Норвегії. В першу чергу це пов’язано з локдауном – його впровадження допомогло Норвегії не зазнати великої кількості захворювань, тоді як Швеція навпаки, через ігнорування карантинних заходів зазнала зріст рівня захворюваності. Це вплинуло і на

зріст рівня безробіття – Норвегія в перші місяці запровадила карантинні заходи, що допомогло в майбутньому не впроваджувати їх знову, зберігаючи при цьому велику кількість робочих місць. В Швеції ж не впровадження локдауну тільки погіршило ситуацію з безробіттям в майбутньому.

Список використаних джерел:

1. Unemployment by sex and age – monthly data. URL: https://ec.europa.eu/eurostat/cache/metadata/en/une_rt_m_esms.htm
2. Data on COVID-19 (coronavirus) by Our World in Data. URL: https://github.com/owid/covid-19-data/tree/master/public/data/

Науковий керівник: доцент Бойко В.Д.

ДЕЯКІ ОСОБЛИВОСТІ АНАЛІЗУ ПРАЦЕЗДАТНОСТІ КОМПОНЕНТІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Задерейко О.В.

кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Для підвищення ефективності аналізу характеристик цифрових пристроїв на практиці використовується імітаційне моделювання їх цифрових компонентів. Цей процес виконується з використанням різних методів моделювання, які набули особливого поширення в сучасних умовах [1].

Особливості моделювання цифрових пристроїв

Метод цифрового моделювання електронних схем є одним з найпоширеніших способів тестування компонентів цифрових пристроїв. Він має ряд істотних переваг перед іншими технологіями [2]: гнучкість управління у постановці експериментів; можливість обліку початкових і кінцевих умов; великий діапазон представлення вхідних величин; висока точність розрахунків.

При цифровому моделюванні в роботі цифрових схем розкриваються недоліки і помилки проектування і режимів експлуатації.

Метод аналогового моделювання електронних схем зазнав значний розвиток і у сучасних реаліях має важливі переваги [3]: проста генерація різних форм вхідних сигналів; визначення стану динамічних систем.

Аналогове моделювання засноване на експериментальному впливі і подальшої реєстрації несприятливих факторів: постійного/змінного струму; шумів і перехідних процесів; зміни їх значень і параметрів.

Методи цифрового і аналогового моделювання однаково затребувані при створенні цифрових електричних схем і вузлів комп'ютерної техніки. Тому

з'явився комбінований метод – цифроаналогове моделювання, що поєднує в собі переваги обох методів. Це дає наступні можливості розробнику:

- докладний аналіз проєктованого цифрового пристрою;
- оптимальний підбір налаштувань для тестування цифрового пристрою;
- точна оцінка отриманих результатів.

Цифроаналогове моделювання електричних схем дозволяє отримати швидкий та точний результат. Параметри цифрових сигналів відслідковуються спеціалізованими засобами в режимі реального часу в один його проміжок.

Основною проблемою при моделюванні динамічних цифрових систем є розробка їх моделей, адекватних реальним процесам, що відбуваються в цифрових системах з прийнятною похибкою.

Динамічні характеристики цифрових пристроїв

Фактично будь-який цифровий пристрій можна уявити як динамічну систему, яка характеризується своїм станом - сукупністю характеристик протягом необхідного проміжку часу [4].

Ідеальні і реальні компоненти цифрових пристроїв являють собою їх узагальнені властивості, втілені в їх цифрові моделі. До них відносяться різні первинні електричні компоненти, такі як резистори, транзистори, діоди, і джерела напруги з ідеалізованими характеристиками. Шляхом вибору невеликого числа чітко визначених параметрів компонентів можна диференційовано описати властивості цифрових компонентів з використанням еквівалентних схем і отримати адекватні моделі ідеальних та реальних компонентів для аналізу досить складних цифрових пристроїв.

Важливим аспектом при побудові моделей динамічних цифрових систем є визначення залежностей і коефіцієнтів у рівняннях, що використовуються при побудові їх моделей.

Для оцінки динамічних характеристик цифрових компонентів цифрової електроніки була використана система схемо-технічного моделювання Multisim [5]. Її можливості дозволяють виконувати аналіз схем на постійному (DC) і змінному (AC) струмі. При DC аналізі визначається робоча точка схеми в сталому режимі роботи. Його результати можуть бути відображені за допомогою приладів, таких як вольтметр і амперметр. AC аналіз використовує результати DC аналізу для отримання лінеаризованих моделей нелінійних компонентів. AC аналіз схем може виконуватися як у часовій, так і в частотній областях.

В системі схемо-технічного моделювання Multisim існує можливість дослідження перехідних процесів при впливі на схеми вхідних сигналів різної форми. Він дозволяє виконувати аналіз цифро-аналогових і цифрових схем великої міри складності. Наявні в програмі бібліотеки включають в себе великий набір широко поширених цифрових компонентів. Є можливість підключення і створення нових бібліотек компонентів. Великий набір приладів дозволяє проводити вимірювання різних величин, задавати вхідні впливи, будувати графіки. Відмінною особливістю цієї системи є наявність ідеальних і реальних моделей цифрових

компонентів та їх складових, що значно спрощує процес перевірки працездатності цифрових пристроїв та подальшої процедури налагодження їх робочих режимів експлуатації.

Динамічні характеристики реальних і ідеальних електронних компонентів

Динамічні характеристики цифрових компонентів (швидкодію) прийнято оцінювати середнім часом затримки розповсюдження сигналу $t_{зат.}$ [6]. Його визначають за формулою

$$t_{зат.} = (t_{10} + t_{01})/2, \quad (1)$$

Тут t_{01} – час затримки розповсюдження при перемиканні зі стану логічного нуля в стан логічної одиниці; t_{10} – час затримки розповсюдження при перемиканні з стану логічної одиниці в стан логічного нуля. Час затримки поширення вимірюють зазвичай на рівні 0.5 від повної амплітуди вхідного і вихідного імпульсів (рис. 1).

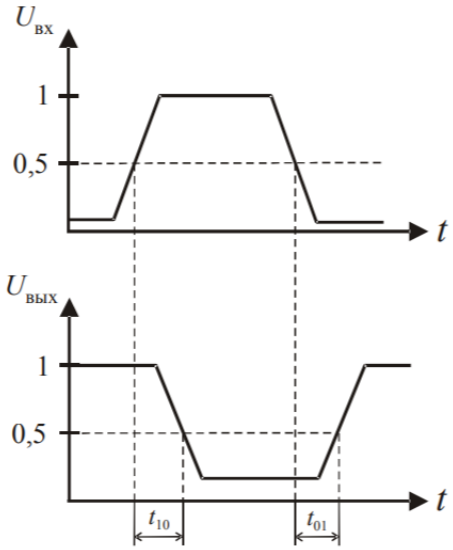


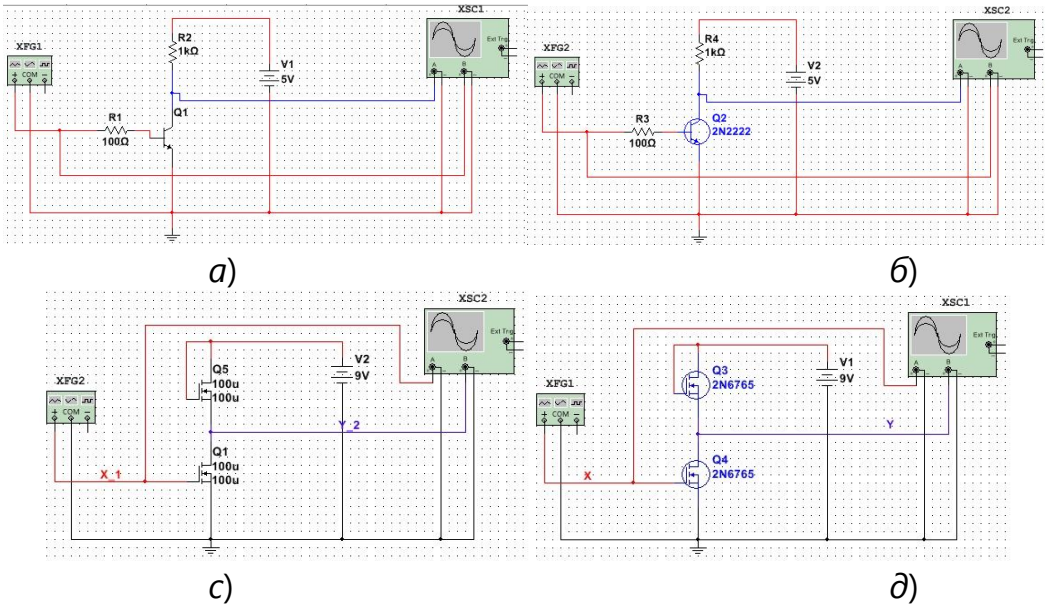
Рис. 1. Затримка поширення вихідного сигналу t_{01}, t_{10}.

Оскільки тривалість перехідного процесу із стану «1» → «0» і «0» → «1» залежить від характеру навантаження, час затримки розповсюдження оцінюють, вважаючи, що цифровий логічний елемент навантажений вхідний ланцюгом такого ж елемента, що має, звичайно, високий вхідний опір [7].

Для дослідження динамічних характеристик було використано найпростіший логічний інвертор. Мета дослідження полягала у визначенні різниці затримки $t_{зат.}$ між моделями ідеального і реального логічного інвертора на біполярних транзисторах і на МОН транзисторах (рис. 2).

Результати моделювання динамічних характеристик принципових схем логічного інвертора (рис.2, *а*; рис.2, *б*), наведені на рис. 3.

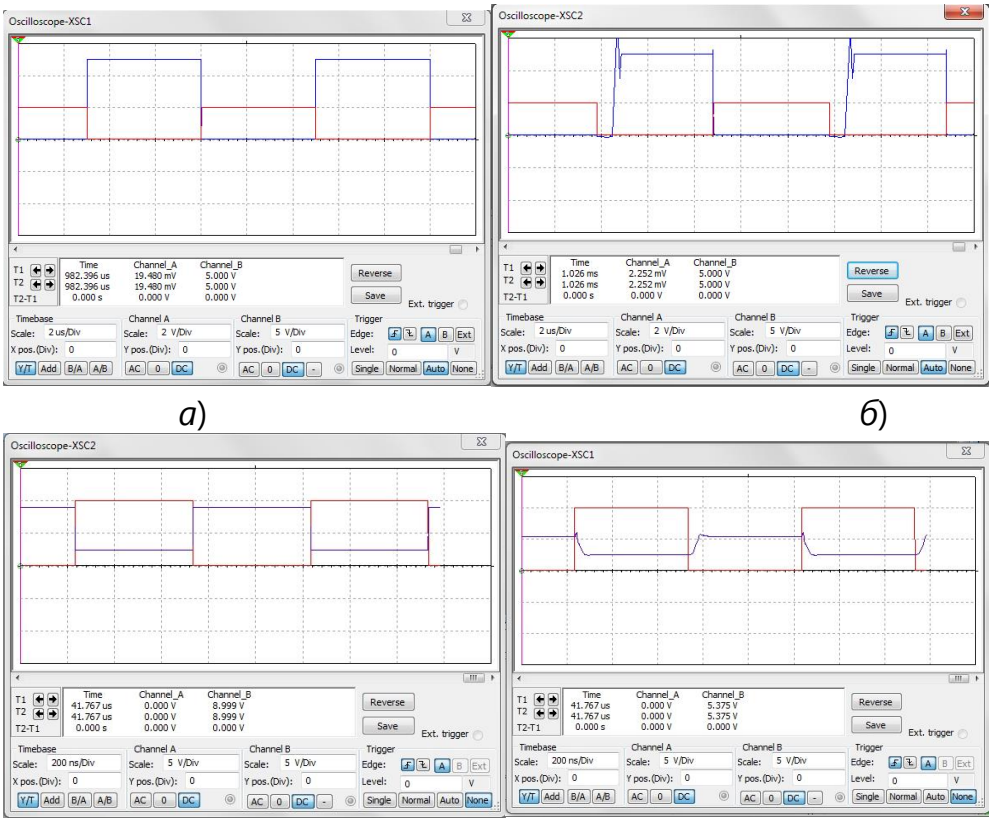
Як видно з рис.3, *б*, передній фронт сигналу на виході реального біполярного транзистора має автоколивальний характер і має деяку затримку по відношенню до заднього фронту вхідного сигналу.



а) *б*)

с) *д*)

Рис. 2. Принципова схема логічного інвертора: а) на біполярному ідеальному транзисторі; б) на біполярному реальному транзисторі; *с*) на МОН ідеальному транзисторі; *д*) на МОН реальному транзисторі.



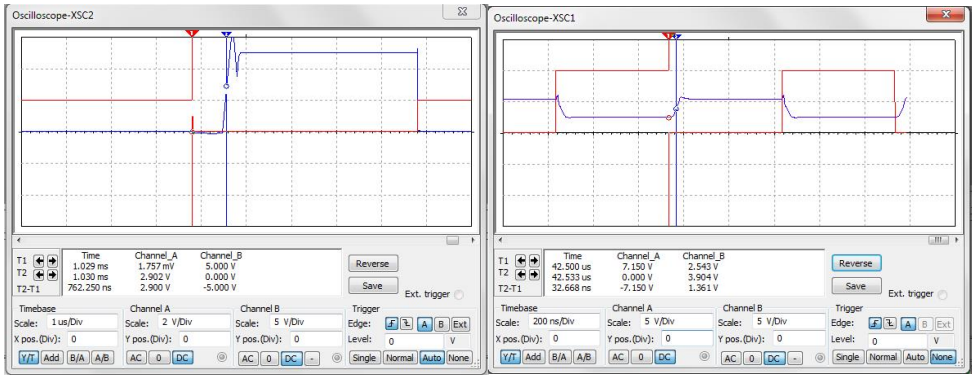
а) *б*)

с) *д*)

Рис. 3. Динамічні характеристики логічного інвертора: *а*) на біполярному ідеальному транзисторі; *б*) на біполярному реальному транзисторі; *с*) на МОН ідеальному транзисторі; *д*) на МОН реальному транзисторі.

Як видно з рис.3, *д*, передній фронт сигналу на виході реального МОН транзистора має менш виражений автоколивальний характер і також має меншу затримку по відношенню до заднього фронту вхідного сигналу.

Визначимо експериментально реальний час затримки перемикання логічного інвертора на біполярному та МОН транзисторах (рис. 4).



а) *б*)

Рис. 4. Тимчасова затримка сигналу на виході логічного інвертора:
а) на біполярному реальному транзисторі; *б*) на МОН реальному транзисторі.

Тимчасова затримка $t_{зад.бп.}$ = 762,25 Нс (рис.4, *а*) на виході логічного інвертора реалізованого на реальному біполярному транзисторі. Тимчасова затримка $t_{зад.мон.}$ = 36,67 Нс (рис.4, *б*) на виході логічного інвертора реалізованого на реальному МОН транзисторі. При цьому на виході логічного інвертора на ідеальному біполярному і МОН транзисторах (рис. 3, *а*; рис. 3, *с*) затримка вихідного сигналу і якісь зміни його форми відсутні.

Висновки

В результаті виконаного дослідження було встановлено, що для досягнення заданої адекватності результатів моделювання цифрових пристроїв, принципове значення має використання реальних елементів в модельованих цифрових пристроях. Це пояснюється максимальною наближеністю одержуваних результатів моделювання до реальних режимів експлуатації логічних елементів на біполярних та МОН транзисторах.

Затримка вихідного сигналу логічного інвертора на МОН транзисторі $t_{зад.мон.}$ менша у ≈ 21 разів порівняно з затримкою вихідного сигналу логічного інвертора на біполярному транзисторі $t_{зад.бп.}$. Це наочно підтверджує більш переважне використання МОН транзисторів у цифрових пристроях.

Список використаних джерел:

1. Цифрова схемотехніка. Моделювання та аналіз. Видання друге, виправлене та доповнене. [Електронний ресурс]: навч. посіб. для студ. спеціальності 171 "Електроніка" / КПІ ім. Ігоря Сікорського; уклад.: В.В. Макаренко, В.М. Співак. Електронні текстові дані (1 файл: 16,3 Мбайт). Київ: КПІ ім. Ігоря Сікорського, 2021. 490 с.

2. Y. Gao, H. Lv, Y. Hou, J. Liu and W. Xu, "Real-time Modeling and Simulation Method of Digital Twin Production Line," *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, 2019, pp. 1639-1642, doi: 10.1109/ITAIC.2019.8785703.
3. S. Tian, C. Yang, F. Chen and Z. Liu, "Circle Equation-Based Fault Modeling Method for Linear Analog Circuits," in IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 9, pp. 2145-2159, Sept. 2014, doi: 10.1109/TIM.2014.2307993.
4. Багацький, В. О. Передавальні характеристики елементів аналого-цифрових пристроїв. *Комп'ютерні засоби, мережі та системи*. 2002, №1. С. 45 – 52.
5. Бурячок В. Л., Коршун Н. В., Шевченко С. М., Складанний П. М. Застосування середовища ni multisim при формуванні практичних навичок студентів спеціальності 125 «Кібербезпека». № 1(9), 2020, С. 159 – 169.
6. Коваль, А. О. Динамічні характеристики засобів вимірювальної техніки. Підручник, Харків, 2019, 211 с.
7. Філенюк, М. А., Ліщинська Л. Б., Войцеховська О. В., Стахов В. П. Моноімітансний логічний R-елемент HI. *Інформаційні технології та комп'ютерна інженерія*, № 2, 2015, С. 71-76.

ОСОБЛИВОСТІ БІБЛІОТЕКИ SFML У МОВІ C++

Коледа С.С.

студент 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Simple and Fast Multimedia Library (SFML) — це кросплатформна бібліотека для розробки програмного забезпечення, яка забезпечує простий інтерфейс прикладного програмування (API – aplication programming interface) для різних мультимедійних компонентів [1].

Бібліотека SFML написана мовою C++ із доступними прив'язками для більшості найвідоміших мов програмування, безкоштовна для будь-якого використання: комерційного чи особистого, власного або з відкритим кодом, тому її можна використовувати без будь-яких обмежень [2].

Основними можливостями бібліотеки SFML є:

1. *Кросплатформність:* наявність можливості компілювання на платформах типу Windows (98, 2000, XP і Vista) і Unix системах (Linux і Mac OS X). З розвитком бібліотеки додаватимуться інші платформи.

2. *Об'єктно-орієнтованість:* надає ефективну об'єктно-орієнтовану модель, яка заснована на стандартних шаблонах та ідіомах, що забезпечує простоту та надійність системи.

3. *Легкість у використанні:* SFML націлена на легке керування. Зроблено упор на найбільш прості публічні інтерфейси.

4. *Гнучкість:* Замість одного великого API, містить декілька модулів (System, Window, Graphics, Sound, Network), які можуть бути вибрані та скомбіновані

залежно від можливого використання. Існує можливість використання лише базового пакету Window для керування вікнами та введенням, а також повний графічний пакет Graphics зі спрайтами та пост ефектами.

5. *Легка інтегрованість:* існує можливість використання в одному або декількох вікнах, а також може бути вбудованою до компонентів інтерфейсу компілятора. Інтеграція з існуючими бібліотеками графічного інтерфейсу користувача GUI (Graphical User Interface – графічний користувальницький інтерфейс система засобів для взаємодії користувача з електронними пристроями, заснована на поданні всіх доступних користувачеві системних об'єктів і функцій у вигляді графічних компонентів екрану) дозволяє додати відображення бібліотеки SFML у складні інтерфейси, побудовані за допомогою Qt, wxWidgets, MFC та ін. [3].

Бібліотека SFML складається з декількох модулів, доступних у статичній та динамічній формах:

1. Модуль «*System*» відповідає за портативність, точне вимірювання часу, прості і об'єктно-орієнтовані потоки, та за модуль Unicode для правильної конвертації між UTF та локально-залежними кодуваннями;

2. Модуль «*Window*» використовується як мінімальний, переносимий пакет для заміни GLUT (OpenGL Utility Toolkit – це незалежний від віконної системи інструментарій для написання програм на OpenGL. Він реалізує простий віконний інтерфейс прикладного програмування API для OpenGL) або SDL (Simple DirectMedia Layer – це вільна кросплатформена мультимедійна бібліотека, що реалізує єдиний програмний інтерфейс до графічної підсистеми, звукових пристроїв і засобів введення для широкого спектру платформ. Дана бібліотека активно використовується при написанні кросплатформених мультимедійних програм). Реалізує організацію вікон і введення з OpenGL. Дає можливість створювати кілька вікон візуалізації, надає інтерфейси для обробки введення. Забезпечує підтримку миші (до п’яти кнопок) та джойстиків (до семи осей та 32 кнопок).

3. Модуль «*Graphics*» надає доступ до простих інтерфейсів OpenGL, сучасних ефектів з апаратним прискоренням: альфа-змішування, обертання, шейдери та інше. Забезпечує ефективне управління пам'яттю, завантажування та зберігання зображення стандартних форматів: BMP, DDS, JPEG, PNG, TGA та PSD. Надає можливість використовувати огляд, подібний до 3D-сцени, для масштабування / переміщення / обертання всього світу. Підтримує спрощену мови шейдерів, яка використовується для додавання пост-ефектів у реальному часі та забезпечує роботу зі шрифтами.

4. Модуль «*Sound*» дає можливість завантажувати та зберігати звуки стандартних форматів: Ogg, WAV, FLAC, AIFF, Au, RAW, paf, 8SVX, NIST, VOC, IRCAM, W64, MAT4, MAT5 PVF, HTK, SDS, AVR, SD2, Core Audi, MPC2K, RF64. Забезпечує роботу технології 3D звуку. Додає простий інтерфейс для захоплення звуку, підтримку потокової передачі даних для великих файлів та підтримка багатоканальних форматів (моно, стерео, 4.0, 5.1, 6.1, 7.1).

5. Модуль «*Network*» реалізує портативний шар над TCP та UDP сокетами та просту передачу даних за допомогою пакетів. Додає класи для використання HTTP та FTP протоколів [1, 2].

Бібліотека SFML має такі недоліки:

1. Не призначена для роботи з 3D графікою, тому що вона створена для забезпечення низькорівневого апаратного прискорення *2D* - графіки. Для її застосування з 3D графікою доведеться використовувати в поєднанні з OpenGL.

2. Недопрацьована підтримка операційних систем Android та iOS. Незважаючи на існування експериментальних версій, наразі стійкої підтримки для Android, iOS чи інших мобільних платформ немає [5].

Отже, бібліотека SFML є оптимальним інструментом для реалізації 2D мультимедійних проектів. Особливо для роботи з мовою C++, SFML – це найбільш чудовий вибір. Однак, вона не відрізняється великим спектром використання, й здебільшого поступається своїм функціоналом бібліотеці OpenGL.

Список використаних джерел:

1. A Closer Look at SFML. URL: https://gamefromscratch.com/a-closer-look-at-sfml/
2. SFML Graphics Library | Quick Tutorial URL: https://www.geeksforgeeks.org/sfml-graphics-library-quick-tutorial/
3. SFML URL: https://github.com/SFML/SFML
4. SFML FAQ URL: https://www.sfml-dev.org/faq.php#grl-whatis/
5. SFML URL: https://ru.stackoverflow.com/tags/sfml/info/

Науковий керівник: доцент Задерейко О.В.

ЩОДО ЗАСТОСУВАННЯ ТЕОРІЇ НЕЧІТКИХ МНОЖИН У КОНТРОЛЕРАХ СИСТЕМ «РОЗУМНИЙ БУДИНОК»

Кулешова Є.Р.

лаборант кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Розвиток людства було в значній мірі обумовлено інноваціями, розширеннями розповсюдженням нових технологій, які відіграють важливу роль в сучасному суспільстві, посиленням соціального добробуту і визначення нових способів взаємодії людей з навколишнім середовищем. У минулому столітті люди зробили гігантський ривок в розвитку багатьох сфер діяльності людства. Природно, цей прогрес був обумовлений масштабним впровадженням технологій.

В останні роки, розумний будинок - це нова парадигма, яка дозволяє людям усвідомлено управляти домашніми енергоресурсами і мінімізувати нераціональне витрачання різних енергетичних ресурсів. Ця концепція, яка може бути відповіддю на виклики, викладені вище, придбала важливість завдяки чотирьом факторам [1]:

- швидкий прогрес і мініатюризація, що спостерігаються в сфері напівпровідникових технологій, що призводять до поширення обчислювальних і електронних пристроїв в нашому повсякденному житті;
- експоненціальне зростання обчислювальної потужності блоку мікроконтролерів (MCU);
- інтеграція вдосконаленого формування сигналу в дуже маленькі сенсорні вузли, які можуть вимірювати і зберігати дані, використовуючи складні методи обробки;
- швидкий розвиток і прогрес бездротових технологій, в основному малої дальності і малої потужності.

Вимоги до створення системи «розумний будинок» не можна чітко визначити і зробити їх універсальними, оскільки в кожного власника вони дещо відрізняються, що викликає певні труднощі в процесі її реалізації та обумовлює необхідність постійного вдосконалення, налаштування і програмування певних функцій.

Аналізуючи статистику проведених опитувань різних міжнародних видань, можна сформувати перелік вимог власників помешкань, які очікуються від системи «розумний будинок» та їх значущість [2]:

- зручність – 30%
- простота використання – 17%
- центральне управління – 10%
- надійність – 8%
- задоволення/розваги – 8%
- комфорт – 8%
- вартість/якість – 6%
- естетика/зовнішній вигляд – 5%
- економія – 4%
- безпека – 3%
- сервіс – 1%

З наведеної статистики можна зробити висновок, що найбільші очікування від системи «розумний будинок» пов’язані з комфортом проживання, а вимога економії енергоносіїв займає лише дев’яте місце. Така ситуація справедлива для закордонних власників систем «розумний будинок».

Стосовно України, більша частина споживачів встановлює системи «розумний будинок» передусім для зменшення витрат енергоносіїв, а вже потім – для забезпечення комфорту та підтвердження свого статусу. Розробники та постачальники таких систем, як правило, мають певний базовий комплект для реалізації системи інтелектуального будинку і пропонують встановити його власнику будівлі.

Що стосується деяких методів, які застосовуються у програмному забезпеченні, на наш погляд, особливої уваги заслуговує застосування нечіткої логіки.

Найбільш важливим застосуванням теорії нечітких множин є контролери нечіткої логіки. Їх функціонування дещо відрізняється від роботи звичайних контролерів; для опису системи замість диференційних рівнянь використовуються знання експертів. Ці знання можуть бути виражені за допомогою лінгвістичних змінних, які описані нечіткими множинами.

Алгоритми нечіткої логіки можна застосовувати, наприклад, для визначення комфортних умов перебування в системах «розумного будинку». Одним з таких напрямів є обчислення комфортних температур.

Реалізація системи оцінювання передбачає три основні етапи [3]:

- визначення лінгвістичних змінних, базових терм-множин, функції належності;
- визначення правил нечітких висновків;
- процес дефазифікації.

Ці етапи схематично зображено на рис. 1.

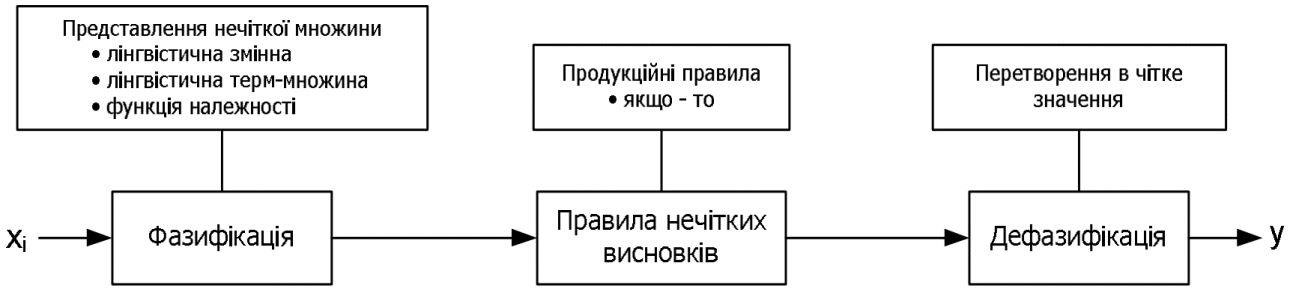


Рис. 1. Модель нечіткої логіки в системі оцінювання

Результат, отриманий після оцінювання нечітких правил, зазвичай є нечітким значенням. Функцію належності використовують для перетворення нечіткого виходу на чітке значення. Цей процес називається дефазифікацією. Одним з методів, які для цього застосовують, є метод середнього центру або центроїдний метод.

Ця методика дозволяє за допомогою оцінювання внутрішньої і зовнішньої температури повітря з використанням правил нечіткої логіки визначити, як потрібно скорегувати температуру до комфортних значень.

Результати цих досліджень можуть бути застосовані в системах управління «розумними будинками», що значно спростить процес розробки, розширення та підтримки таких систем, а також покращить рівень безпеки процесу управління "розумними будинками" та наддасть змогу гнучко запровадити інтелектуальні пропозиції по управління Розумними Будинками користувачам на основі побудованих на їх індивідуальних даних профілів комфорту користувачів.

Подальші дослідження цієї теми слід вести в напрямку проведення випробувань напрацьованих підходів на реальному апаратному забезпеченні зперевіркою повноцінної працездатності цих підходів під час реального використання системи як «розумного будинку».

Список використаних джерел:

1. Guangyi Xiao, Member, IEEE, Jingzhi Guo, "User Interoperability With Heterogeneous Iot Devices Through Transformation" // IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 10, NO. 2, MAY 2014.
2. Y. N. Hassan, G. Ramanathan, and M. Kovatsch, "Demo: developing smart environments in the internet of things with the semantic IDE," //Proceedings of 2015 5th International Conference on the Internet of Things (IoT), Seoul, Korea, 2015, pp.1
3. «Побудова моделі оцінювання параметрів теплового комфорту на основі нечіткої логіки 2010./ Машевська М., Ткаченко П. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/8270/1/141pdf.

Науковий керівник: доцент Чепурна О.Є.

СКАНДАЛ BATTARYGATE

Латиш Я. В.

студентка 1 курсу факультету міжнародно-правових відносин Національного університету «Одеська юридична академія»

Компанія Apple завжди знаходиться в центрі уваги та на вершині технологічний інновацій. Проте єдиний конфлікт, який коштував їй мільйони доларів, була афера з батареєю.

«Apple приховувала інформацію про те, що батареї знижували продуктивність телефонів iPhone, видаючи це за оновлення» – саме с такою скаргою люди масово почали звертатися до служб підтримки [1].

На початку 2016 року старі iPhone почали стикатися з проблемами надійності, такими як раптове вимкнення, це відбувалося коли їх ємність акумулятора досягла порогу в 30 відсотків. Це було викликано падінням напруги на клемах акумулятора, який був нижче рівня, необхідного для роботи телефону. У відповідь на незадовільні запити і численні скарги компанія Apple заявила, що ця проблема стосується лише невеликої кількості телефонних пристроїв.

Подібні проблеми з обладнанням не є чимось новим у цій галузі, оскільки виробники електроніки вже на стадії проектування пристроїв закладають у конструкцію певний «запас міцності», обмежуючи реальний термін їх експлуатації лише кількома роками.

Така бізнес-стратегія дістала назву «заплановане старіння». При цьому виробнику заздалегідь відомо, через який термін користувачам потрібно замінити пристрій на новий. Електронні пристрої можуть працювати без проблем до 10 років, але такий тривалий термін не влаштовує виробників, оскільки призводить до зниження продажів нових пристроїв.

Apple навмисно уповільнювала роботу старих пристроїв. Компанія, звичайно ж, усвідомлювали, як це вплине на продажі. Зрозуміло, що багато

користувачів вирішили, що єдиний спосіб підвищити продуктивність пристрою - купити iPhone більш нової моделі.

Зрештою, Apple довелося визнати ці проблеми, і принести клієнтам офіційні вибачення, написавши: «Ми знаємо, що деякі з вас вважають, що Apple вас підвела. Ми вибачаємося». Однак багато клієнтів визнали, що одних вибачень недостатньо і зажадали провести безкоштовну заміну акумуляторів.

У 2017 року Apple оновила iOS 10.2.1, тобто були внесені зміни на всіх пристроях, новіших за iPhone 6. До кінця року Apple оприлюднила публічну заяву про те, що вона нібито «задушила» процесор через старі батареї, що призвело до масового суспільного резонансу та багатьох людей, які подали позови. Щоб врятувати свою компанію від падіння, Apple обрала проміжний варіант вирішення цього питання та надала значну знижку на послугу заміни акумуляторів для iPhone 6 і новіших моделей на 2018 рік, що, зрештою, коштувало їй 11 мільйонів доларів [2].

Через деякий час Apple випустила ще одне оновлення iOS 11.3, яке забезпечило покращення стану батареї. Для контролю пошкоджень і для того, щоб уникнути погіршення ситуації, клієнти, які оплатили поза гарантійну заміну батареї для iPhone 6 або старіших пристроїв у 2017 році, в кінцевому підсумку отримали відшкодування у розмірі 50 доларів.

Після цього компанія звернулася до федеральних суддів з проханням відхилити позов проти них щодо цієї справи, оскільки технічно вони вже «заплатили ціну».

Згідно з умовами попередньої угоди про груповий позов на суму 500 мільйонів доларів, будь-який нинішній або колишній власник iPhone 6 або 7 може отримати виплату приблизно в 25 доларів від Apple, тоді як деякі названі члени класу можуть отримати 1500 або 3500 доларів [3].

Така компанія, як Apple, завжди знаходиться під пристальною увагою громадськості, тому шахрайство з батареєю було однією з найгірших і найдорожчих помилок, з якими стикалася будь-яка компанія.

Таким чином, урок, який ми всі можемо винести зі скандалу, полягає в тому, щоб ніколи не ставити мету здобування грошей понад потреби споживачів. Ця афера призвела до того, що Apple втратила не тільки репутацію, але й мільйони доларів у вигляді компенсації та штрафів у більш ніж одній країні.

Список використаних джерел:

1. James Clayton Apple to pay $113m to settle iPhone 'batterygate' URL: http://surl.li/byfnq.
2. Rachel Sandler Apple Settles ‘Batterygate’ Lawsuit For $113 Million URL: http://surl.li/byfnk.
3. Eli Moskowitz Apple to Pay $113 Million Settlement Over ‘Batterygate’ Scandal URL: http://surl.li/byfnd.

Науковий керівник: доцент Чанишев Р. І.

ОСОБЛИВОСТІ ПІДГОТОВКИ ДАНИХ З МЕТОЮ ПОДАЛЬШОГО АНАЛІЗУ

Лобода Ю. Г.

кандидат педагогічних наук, доцент,
доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Підготовка даних – це процес їх об'єднання, приведення до єдиного формату, очищення з метою подальшого аналізу даних та вирішення інших бізнес-завдань. Підготовка даних – це компонент багатьох корпоративних систем та програм, що обслуговуються IT-відділом, таких як системи зберігання даних та бізнес-аналітики. Однак підготовлені дані потрібні бізнес-користувачам і для інших цілей, наприклад, для аналізу та складання разових звітів.

Як наслідок IT-фахівці та інші співробітники, наприклад, фахівці з дослідження даних, змушені обробляти безліч запитів на підготовку спеціальних наборів даних. У наші дні зростає інтерес бізнес-користувачів до інструментів самостійної підготовки даних, що дозволяє отримувати доступ до джерел інформації та працювати з ними.

Особливості підготовки даних: пошук, утримання, очищення, документування та доставка.

1. Пошук. Суть цього етапу – пошук даних, які найбільше підходять для вирішення конкретного завдання. Для ефективного пошуку даних необхідно створити та підтримувати повний, грамотне задокументований каталог даних (тобто репозиторій метаданих). Крім статистики з профілювання даних та іншого вмісту, в каталозі зберігається описовий індекс, що вказує на розташування доступних даних.

Профілювання даних - це ключ до їх розуміння, оскільки воно забезпечує високорівневу статистику за якістю даних (кількість рядків, типи даних у стовпцях, мінімальні, максимальні та середні значення по стовпцях, кількість нульових значень тощо). Профілювання полегшує вибір одного з кількох відповідних наборів даних [1].

При пошуку важливо не тільки знайти дані, які необхідні прямо зараз. Слід також передбачити можливість їхнього повторного пошуку пізніше, коли знову виникне така потреба. При використанні нових джерел інформації, особливо зовнішніх, потрібно оновлювати каталог даних.

2. Утримання. Суть етапу утримання – консолідація даних, відібраних на етапі пошуку. В багатьох організаціях дані залишаються "за ґратами" електронних таблиць надовго, навіть коли підготовка завершена. На етапі очищення потрібний тимчасовий робочий простір або зона тимчасового зберігання даних [2]. Щоб безперервно утримувати проміжні або доставлені дані, потрібно використовувати загальне та кероване сховище: реляційну базу даних, мережну

файлову систему або репозиторій великих даних, наприклад, озеро даних на платформі Hadoop . Новим віянням є розміщення даних безпосередньо в оперативній пам'яті (або хмарі). Це значно прискорює процеси консолідації і приведення даних до потрібного формату, що передують подальшій обробці.

3. Очищення. Очищення використовується і для оцінки якості даних і тому є невід'ємною частиною їх підготовки. Трудомісткість цієї оцінки (вона зазвичай включає перевірку, дедуплікацію та збагачення даних) часто залежить від можливості повторного використання компонентів з інших розгорнутих систем.

Так, наприклад, у сховищах даних та системах бізнес-аналітики виконується перетворення та оцінка якості даних при інтеграції безлічі джерел даних у єдину модель, оптимізовану для обробки запитів та підготовки стандартних звітів [3].

Крім того, під час процесу очищення можна фільтрувати та агрегувати дані, щоб створювати власні уявлення або презентації з різним рівнем деталізації. Деякі аналітичні інструменти дозволяють реалізувати функцію очищення безпосередньо в оперативній пам'яті, щоб запобігти постійному зберіганню альтернативних уявлень доставлених даних.

4. Документування. Документування – це процес запису бізнес- та технічних метаданих про знайдені, консолідовані та очищені дані. До метаданих відносяться: технічні описи; бізнес-термінологія; інформація про походження даних до джерела; історія змін, внесених під час дистиляції; зв'язки з іншими даними; рекомендації щодо використання даних; пов'язані правила керування даними; ідентифіковані адміністратори основних даних.

Всі ці метадані доступні у каталозі даних. Підготовка даних вручну, зазвичай в електронних таблицях, - не тільки трудомісткий, але й процес, що часто дублюється. Це пояснюється тим, що різні користувачі (або навіть одна людина) можуть отримувати різні результати при вирішенні однієї і тієї ж задачі. Загальні метадані дозволяють прискорити підготовку даних та послідовно повторити її за необхідності. Крім того, завдяки спільним метаданим можуть ефективно співпрацювати кілька користувачів, які відповідають за різні аспекти підготовки даних [3].

5. Доставка. Доставка – це приведення очищених даних до формату, придатного для використання людиною чи процесом. При цьому необхідно оцінювати потребу у постійному утриманні доставлених наборів даних. Якщо вона є, то відповідні метадані поміщають у каталог, щоб інші користувачі могли шукати дані.

При доставці необхідно дотримуватися політик управління даними, щоб, наприклад, мінімізувати ризик витоку конфіденційної інформації. Важливо відзначити, що доставка буває не лише одноразовою. У разі доставок нових або змінених даних, що повторюються, підготовка виконується за розкладом або запитом. Крім того, необхідно відстежувати використання доставлених даних, а невикористовувані - видаляти через певний час (разом із відповідними записами в каталозі даних) [4].

Завдяки загальним метаданим, постійно керованому сховищу та логіці багаторазового перетворення та (або) очищення підготовка даних перетворюється на ефективний, послідовний та повторюваний процес. Своєю чергою треба знаходити релевантні дані та озброюватися знаннями, необхідними для швидкого використання даних на практиці.

Для оптимізації роботи потрібно подбати про те, щоб усі процеси підготовки даних можна було легко застосовувати повторно і розгортати в операційних системах і на виробничих об'єктах. Завдяки підготовці даних (пошуку, утриманню, очищенню, документуванню та доставці) можливо максимально ефективно використати інформаційні активи.

Список використаних джерел:

1. Papenbrock, Thorsten. Data profiling - efficient discovery of dependencies (2017) URL: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/40670/file/ papenbrock_diss.pdf
2. Консолідація облікової інформації в управлінні діяльністю підприємств та їх об'єднань: монографія: [Електронне видання] / А.А. Пилипенко, Ю. Д. Маляревський, Л. В. Безкоровайна та ін. ; за заг. ред. д-ра екон. наук, професора А. А. Пилипенка. Харків : ХНЕУ ім. С. Кузнеця, 2016. 319 с.
3. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. 417 с.
4. Теорія та практика моделювання бізнес-процесів: монографія / В.С. Пономаренко, С. В. Мінухін, С. В. Знахур. Х. : Вид. ХНЕУ, 2013. 244 с.

КОМП'ЮТЕРНА ГРАФІКА: ВИКОРИСТАННЯ БІБЛІОТЕКИ OpenGL

Логінова Н. І.

кандидат педагогічних наук, доцент
завідувач кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Янковський О. Г.

кандидат технічних наук, доцент
доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Сучасне використання інформаційно-комунікаційних технологій не можливе без використання елементів комп'ютерної графіки. Це й розробка вебдизайну різних сайтів і створення високоякісних мультимедійних програмних продуктів, комп'ютерних ігор і застосування різноманітних графічних ефектів в анімаційних сюжетах та багато іншого. Тому збільшується потреба в IT-фахівцях, які можуть не тільки розробляти програмні продукти, але й створювати графічні оболонки та реалізовувати дизайнерські задумки за допомогою графічного

програмування. Для набуття знань з програмування графічних зображень й пропонується дисципліна вільного вибору «Комп'ютерна графіка».

В процесі вивчення дисципліни здобувачі вищої освіти знайомляться з основними способами подання графічної інформації, методами обробки графічних зображень. Вивчають основи роботи пристроїв введення та виведення інформації. Опановують основи формування кольорів та використання кольорових моделей. Знайомляться з різними графічними форматами та навчаються конвертувати зображення. Навчаються аналізувати та обирати у відповідності з поставленими задачами інструменти для програмування графічних зображень у сучасних графічних застосунках.

Сучасна комп'ютерна графіка використовує API (Application Programming Interface) – програмний інтерфейс графічних застосунків, тобто програмісти пишуть коди, які викликають функції з попередньо визначеній бібліотеки або наборів бібліотек, що забезпечують підтримку графічних операцій. Існує багато графічних бібліотек, але найпоширенішої є бібліотека OpenGL (Open Graphics Library).

OpenGL – це графічний стандарт в області комп'ютерної графіки, який містить більш 300 функцій для малювання складних 3-х мірних зображень, які складаються з простих примітивів. Використовуються стандарт при створенні комп'ютерних ігор, САПР, створення віртуальної реальності, візуалізації тощо.

Стандарт був розроблений ще у 90-х роках XX століття та нараховує декілька версій від 1.0 до 4.x. Для початкового вивчення програмування елементів комп'ютерної графіки графіки в дисципліні «Комп'ютерна графіка» використовується версія 3.0, оскільки 4.x та модифікована версія Vulkan потрібують від розробників знання з 3D-графіки та системного програмування, вміння розробляти багатопоточні та асинхронні коди.

Характерними особливостями OpenGL є стабільність, надійність та простота у використанні. Зміни, які вносяться до стандарту, реалізуються з урахуванням ранніх версій та є сумісними. Застосунки, які працюють з OpenGL гарантують однаковий візуальний результат, якій не залежить від операційної системи. Стандарт є кросплатформним і підтримує всі сучасні операційні системи – Windows, Linux, macOS. Також OpenGL дозволяє реалізовувати сучасні графічні можливості відеокарт і технологій в області реалістичних зображень, оскільки був спроектований для відеокарт. Стандарт OpenGL гарно структурований та має інтуїтивно зрозумілий інтерфейс, що дозволяє створювати застосунки з меншим числом рядків коду, порівняно з іншими графічними бібліотеками.

OpenGL працює у буфері кадру і для відображення вмісту буферу кадра у вікно екрану застосовують бібліотеки freeglut: CPW, GLOW, GLUI, GLFW та інші. Сучасним варіантом є GLFW (OpenGL Extension Wrangler) – це багатоплатформна бібліотека з відкритим вихідним кодом для програмування комп'ютерної графіки. Вона має простий API для створення вікон, контекстів і поверхонь,

отримання вхідних даних тощо. GLFW написаний на C і підтримує Windows, macOS, X11 і Wayland. GLFW ліцензується за ліцензією zlib/libpng [1].

Програмування комп'ютерної графіки засновано на векторної та лінійної алгебрі. Тому OpenGL супроводжується бібліотекою функцій або пакетом класів для підтримки загальних математичних завдань. Найбільш використаною є GLM (OpenGL Mathematics), яка надає класи та основні математичні функції, пов'язані з графічними поняттями – вектор, матриця та кватерніон. Також вона містить різноманітні допоміжні класи для створення та використання звичайних 3D графічних структур – матриці перспективи та огляду [2].

OpenGL дозволяє додавання текстур до об'єктів у графічних сценах за допомогою різних бібліотек текстур, як FreeImage, DevIL, OpenGL Image (GLI), Glraw і Simple OpenGL Image Loader (SOIL) [3].

Графічне програмування за допомогою OpenGL пов'язане з апаратним і програмним забезпеченням. Використання OpenGL вимагає графічної карти (GPU). Що стосується апаратного забезпечення, OpenGL забезпечує багатоетапний графічний конвеєр, який частково програмується за допомогою мови GLSL (OpenGL Shading Language). З боку програмного забезпечення API OpenGL написаний на C, і є сумісним з C і C++, а також доступна для інших мов програмування: Java, Perl, Python, Visual Basic, Delphi, Ruby тощо [4].

Дисципліна «Комп'ютерна графіка» викладається на другому курсі та використовує OpenGL на C++, оскільки цю мову програмування здобувачі вищої освіти вивчають на першому курсі в дисципліні «Алгоритмізація та програмування».

OpenGL є універсальним інструментом для програмування графічних зображень. Знання, здобути на заняттях з дисципліни «Комп'ютерна графіка» будуть корисними при створенні різних засобів візуалізації програмних продуктів.

Список використаних джерел:

1. GLFW. URL: https://www.glfw.org
2. OpenGL Mathematics (GLM). URL: http://glm.g-truc.net/0.9.8/index.html
3. Simple OpenGL Image Library 2 (SOIL2), SpartanJ, URL: https://github.com/SpartanJ/SOIL2
4. V. Scott Gordon & John Clevenger. Computer Graphics Programming in OpenGL with C++, 2nd ed. Publisher: David Pallai Mercury Learning and Information, 2021. 535 p.

DATA MINING ЯК НАУКА, ХАРАКТЕРИСТИКА ОСНОВНИХ ВІДМІННОСТЕЙ СПОСОБІВ ВИДОБУТКУ ДАНИХ

Лопаєв Д. В.

студент 1 курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Термін Data Mining більш поширений у повсякденному житті, але іноді його плутають з Big Data. Якщо термін «великі дані» відноситься до постійно зростаючих и оброблених даних, то інтелектуальний аналіз даних – це процес глибокого занурення в ці дані для отримання критичних знань.

Термін «інтелект даних» визначається як процес виявлення в необроблених даних раніше невідомих, важливих, практичних і добре зрозумілих пояснень знань, необхідних для прийняття рішень у різних сферах людської діяльності [1].

Використовуючи програмне забезпечення для пошуку закономірностей у великих пакетах даних, підприємства можуть розробляти маркетингові стратегії, керувати кредитним ризиком, виявляти шахрайство, фільтрувати спам і навіть виявляти настрої користувачів.

Ринок систем аналізу даних зростає. Цьому сприяє діяльність великих корпорацій: SAS, IBM, Microsoft, Oracle та ін. [2]

Існує багато програм, які можуть виконувати завдання аналізу даних. Наприклад, SAS Enterprise Miner, Microsoft Analysis Services, SAS Customer Intelligence 360, SAS Credit Scoring, Board, Sas Revenue Optimization і RapidMiner [3].

Інтелектуальний аналіз даних покладається на ефективний збір, зберігання та комп'ютерну обробку даних. Інтелектуальний аналіз даних вважається окремою дисципліною в галузі науки про дані.

Термін «інтелектуальний аналіз даних» з'явився в академічних журналах ще в 1970 році, але по-справжньому він не прижився до появи Інтернету в 1990-х роках. У той час компаніям потрібно було аналізувати величезні обсяги різнорідних даних, щоб знайти важливі закономірності та навчитися передбачати поведінку клієнтів. Виявляється, що традиційні статистичні моделі не впораються з цим завданням [1].

Останні тенденції аналізу даних включають розвиток методів елементного аналізу віртуальної та доповненої реальності, їх інтеграцію з системами баз даних, вилучення біологічних даних для медичних інновацій, вебмайнінг (аналіз даних в Інтернеті), аналіз даних у реальному часі та захист конфіденційності у діяльності з вилучення даних.

Основною проблемою виявлення шаблонів даних є час, необхідний для пошуку в масиві інформації. Відомі методи або штучно обмежують цей пошук, або

будують ціле дерево рішень, що знижує ефективність пошуку. Вирішення цієї проблеми залишається основною метою розробників продуктів інтелекту даних.

Моделі аналізу даних використовуються для багатьох типів завдань:

- Прогноз: оцінка продажів, прогноз навантаження або простою сервера;
- Ризик і ймовірність: вибір правильних клієнтів для цільових розсилок, визначення балансу сценаріїв ризику, визначення ймовірностей за діагнозом чи іншими результатами;
- Послідовність пошуку: аналіз та вибір клієнтів під час здійснення ними покупок і прогноз їхньої поведінки
- Групування: розподіл клієнтів або події на кластери, аналіз та прогноз загальних характеристик цих кластерів [2].

Аналіз даних має кілька етапів. Перший – формулювання проблеми. Цей крок включає аналіз вимог бізнесу, визначення проблемних областей, оцінку показників моделі та визначення завдань для проекту аналізу. Другий етап – підготовка даних, їх агрегація та очищення. Ця робота передбачає видалення непотрібних даних та визначення джерела найбільш точних даних для створення таблиць аналізу. дослідження даних.

Наступні етапи – дослідження даних, побудова моделі, підтвердження та дослідження цієї моделі, розгортання та оновлення моделей. Після того, як модель запущена, їй потрібно принаймні оновити нові дані, а потім повторно обробити їх.

Видобуток даних в основному використовується в таких споживчих галузях, як роздрібна торгівля, фінанси, телекомунікації, маркетинг, страхування, виробництво, соціологія, медицина та рекомендаційні системи, такі як голосовий помічник Amazon Alexa і Siri від Apple [3].

Список використаних джерел:

1. Data mining in education, Cristobal Romero and Sebastian Ventura. URL: https://onlinelibrary.wiley.com/doi/pdf/10.1002/widm.1075
2. Можливості використання технологій Data Mining при створенні бізнес-проекту, Бондар Є.О. 2019. URL: http://nubip.edu.ua/sites/default/files/zbirnik_10.pdf#page=46
3. Технологія застосування методів Data Mining при розробці рекомендаційних експертних систем для підбору стилю, Литовченко О.В. 2020. URL: https://dspace.nau.edu.ua/handle/NAU/45203

Науковий керівник: доцент Лобода Ю.Г.

АКТУАЛЬНІ ПИТАННЯ ДИСЦИПЛІНИ «АРХІТЕКТУРА ПРОЕКТІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

Манаков С. Ю.

кандидат технічних наук, доцент кафедри інформаційних технологій, Національного університету «Одеська юридична академія»

Архітектура програмного забезпечення має суперечливу репутацію в спільноті Agile [1]. Частково проблема полягає в тому, що архітектура є невдалою метафорою для результату роботи з розробки програмних систем. Натхнене роботою архітекторів-будівельників, слово викликає образи красивих дизайнів, які натякають на утопічне майбутнє. Але робота в галузі архітектури програмних систем набагато динамічніша, ніж це підтримує метафора будівельної архітектури. Будівлі статичні, і робота архітекторів будівель виконується лише один раз. Програмне забезпечення ж за своєю природою є постійно змінним і динамічним.

Аналогія з будівлею змусила деяких архітекторів програмного забезпечення занадто багато зосередитися на структурі та поведінці, а не на рішеннях, які створюють ці структури та поведінку. Справа не в тому, що структура та поведінка є неважливими, але вони є результатами процесу мислення, який важливо зберегти, якщо система хоче стабільно розвиватися з часом. Знати, чому хтось щось зробив, так само важливо, як знати, що він зробив. Те, що вони зробили, повинно бути помітним в коді, якщо він добре організований і прокоментований, але причина часто втрачається. Причина цього в тому, що архітектурні рішення в програмному забезпеченні рідко бувають чіткими. Майже кожне архітектурне рішення є компромісом між конкуруючими альтернативами, і важко побачити переваги альтернатив, доки ви не спробуєте декілька з них і не побачите, як вони працюють.

Це також одна з причин, чому архітектори програмного забезпечення все ще повинні бути розробниками; вони не можуть зрозуміти чи передбачити сили, що діють в системі, не розробивши й не перевіривши щось. Проектування вимагає достатнього знання системи, щоб сформулювати корисні гіпотези щодо атрибутів якості, а також досвіду написання коду та розробки тестів, які можуть оцінити ці гіпотези.

По правді кажучи, використання такої назви, як «архітектор програмного забезпечення», надає неправильне уявлення про характер роботи. Реальність така, що багато розробників програмного забезпечення виконують архітектурну роботу, вони просто не визнають її як таку. Щоразу, коли вони приймають рішення про те, як обробляти атрибути якості, вони впливають на архітектуру системи. Краще усвідомлення того, як неявні рішення впливають на здатність системи досягати цілей якості, є першим кроком у покращенні архітектури системи [2].

Архітектура сучасних програмних застосунків є в своїй основі дослідницькою діяльністю. Команди, які створюють сучасні застосунки, щодня стикаються з новими проблемами: безпрецедентними технічними проблемами [3], а також наданням клієнтам нових способів вирішення нових і відмінних проблем. Це безперервне дослідження означає, що архітектуру не можна визначити наперед, на основі минулого досвіду; команди повинні знайти нові шляхи задоволення вимог до якості.

Як приклад того, що дослідження є важливим для виявлення архітектури, розглянемо наступне: припустимо, що ви є частиною команди, яка працює над програмною системою, спочатку розробленою для обробки структурованих табличних даних, що зберігаються в базі даних SQL. Тепер цю систему потрібно вдосконалити, щоб обробляти неструктуровані дані, включаючи зображення та відео, і очікується, що обсяги значно збільшяться в порівнянні з тими, які зараз обробляє система. Ви розглядаєте можливість додати базу даних NoSQL до свого технологічного стеку для обробки нових типів даних, але оскільки ваша команда не має значного досвіду роботи з цією технологією, необхідно провести експерименти, щоб вибрати правильний продукт бази даних і налаштувати його відповідно до нових вимог до обсягу даних.

Коли команда працює над цими технічними проблемами, вони формують гіпотези про те, які підходи найкраще відповідатимуть їхнім бажаним QAR, які також є припущеннями та змінюватимуться з часом. Вони будують частину рішення для перевірки цих гіпотез і приймають рішення на основі результатів. Сукупним результатом цих рішень щодо відповідності QAR є архітектура системи. Команда може передавати ці рішення різними способами, в тому числі за допомогою документації та діаграм, але документи та діаграми – це не архітектура, а рішення та їхні причини.

Архітектура програмного забезпечення, як дисципліна, потребує оновлення. Її імідж страждає від багатьох старих уявлень про те, які проблеми їй потрібно вирішувати і як вона повинна вирішувати ці проблеми. Розгляд архітектури програмного забезпечення як безперервної діяльності, зосередженої на формуванні гіпотез про те, як система відповідатиме атрибутам якості, а потім використання емпіризму, щоб довести, що система їм відповідає, є сутністю безперервного підходу до архітектури програмного забезпечення. Також потрібно віддалити питання архітектури від людей, які не мають відношення до розробки, і передати її в руки людей, які насправді можуть зробити її реальною та виконаною, – розробників. Тільки тоді стає можливим досягнути високої стабільності, якої вимагають сучасні застосунки.

Список використаних джерел:

1. Len Bass, Paul Clements, Rick Kazman. Software Architecture in Practice. SEI Series in Software Engineering. 3rd edition. 2012. 640 p. ISBN 978-0321815736.

2. Роберт Мартін. Чиста архітектура: мистецтво розробки програмного забезпечення. Вид-во: Фабула. 2019. 416 с. ISBN 978-617-09-5286-8.
3. Марк Річардс. Основи архітектури програмного забезпечення: інженерний підхід. O'Reilly Media. 2020. ISBN 9781492043454.

ТЕНДЕНЦІЇ ВИКОРИСТАННЯ JAVASCRIPT FRAMEWORKS

Мироненко А. А.

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Для того щоб залишатись конкурентоспроможним на ринку IT-праці, кожен працівник IT-індустрії має бути обізнаним із сучасними трендами вебтехнологій. Особливо затребуваними нині на ринку IT-праці є веброзробники. Так, згідно зі статистикою Internet Live Stats нині у світі активними є 1.9 мільярдів вебсайтів [1]. Інтерактивна взаємодія сучасних вебсайтів з користувачами забезпечується засобами вебпрограмування, тому веброзробники мають бути на крок попереду у вивченні тенденцій розроблення функціонального користувальницького інтерфейсу сайтів.

Оскільки бекенд і фронтенд вебсайту реалізуються різними програмними засобами, то до бекенд-програмістів та до фронтенд-програмістів висуваються вимоги володіння відповідними засобами їх розробки. Так, фронтенд-програміст (Front-End Developer / Front-End Programmer), крім верстки, має володіти навичками розробки клієнтських скриптів, наприклад, мовою програмування JavaScript (JS) та знати принаймні один із JavaScript-фреймворків: Vue.js, Angular, React Native, Ember.js, Meteor або Backbone.js [2].

Що стосується мови JavaScript (або JS), наразі вона є однією з найперспективніших мультипарадигмальних мов програмування. За результатами проведеного опитування 2021 року на форумі з програмування Stack Overflow 64,96% з 83 052 опитаних професійних розробників віддали перевагу саме JavaScript [3].

Завдяки використанню наборів бібліотек JS-коду – JavaScript-фреймворків, завдання веброзробника полегшується в рази. Набори різноманітних інструментів цих фреймворків позбавляють програмістів від рутинних дій та суттєво економлять час, оскільки на основі шаблонів дозволяють формувати оптимальний код для розв'язання типових задач веброзробки.

Серед численних JavaScript-фреймворків за результатами опитування, проведеним State of Frontend 2021, в якому взяли участь понад 4,5 тисячі професійних розробників, в трійку найпопулярніших входять [4]:

React – 74,2%;

Angular – 33,4%;

Vue.js – 29,9%.

Для оцінки JS-фреймворків використовують різні підходи та метрики,

наприклад: рейтинг на GitHub, тренди пошуку Google, число завантажувань, яке корелюється з рейтингами пошукових запитів, тощо.

Так, в рейтингу GitHub лідером є Vue.js (понад 195 тисяч зірок) [5]. Vue.js – це JS-фреймворк з відкритим кодом, призначений для спрощення та упорядкованості розробки користувальницького інтерфейсу. Цей прогресивний фреймворк якісно розв'язує типові вебзадачі та швидко інтегрується в проєкт. Завдяки своїй компактності, він по мінімуму навантажує проєкт та дозволяє створювати реактивні та об'ємні застосунки (Single-Page Applications) з серверним рендерингом. Vue.js вважається легким для вивчення, розуміння та використання. Водночас його не використовують для складних багатосторінкових сайтів та бекенду. До того ж, поки що навчальних ресурсів для Vue.js не так багато і підтримка у спільноті вебпрограмістів не така потужна, як для React та Angular. По кількості пошукових запитів в Google Vue.js посідає третє місце [6].

React останні роки є лідером рейтингів кращих JS-фреймворків [7], хоча і посідає лише друге місце в рейтингу GitHub (понад 187 тисяч зірок) [8]. Його використовують такі відомі компанії як: Facebook(meta), Netflix, PayPal, BBC та ін. Серед переваг виділяють наявність численних навчальних курсів та документації. React гнучкий, ефективний, легкий та більш швидкий, ніж Angular, завдяки простій компонентній моделі та функціональності рендерингу на боці сервера. Розробниками React був винайдений проривний в області фреймворків API-інтерфейс під назвою «Hooks», який в перспективі має замінити класи [9]. Ці та інші нововведення, як-от пришвидшення паралельного рендерингу або поліпшення код-сплітінгу, роблять React майже поза конкуренцією. Лідерство React серед усіх JS-фреймворків підтверджується і першістю показника кількості пошукових запитів в Google за останні п'ять років [6].

Angular посідає третє місце в рейтингу GitHub (понад 80 тисяч зірок) [10] і друге місце по кількості пошукових запитів в Google [6]. Цей фреймворк від компанії Google є повнофункціональною інтерфейсною клієнт-платформою з графічним інтерфейсом для розробки вебзастосунків. Angular підтримує зрозумілий для початківців інтерфейс командного рядка та одну з найзручніших серед JS-фреймворків консоль. Серед відмінностей цієї платформи виділяють реактивну компіляцію (до 3 секунд) за допомогою бібліотеки асинхронних операцій – RxJS та вбудовані засоби для тестування застосунку. Angular, на відміну від інших відомих JS-фреймворків, використовує мову програмування TypeScript, для якої характерна сувора типізація, складні типи даних та наявність модифікаторів доступу, що може відштовхувати новачків. Крім того, порівняно з іншими компонентними фреймворками, Angular має значні проблеми з оптимізацією, виникненням інтеграційних помилок при оновленні версії фреймворку та складнощі освоєння даного фреймворку через меншу кількість навчальних курсів і документації, порівняно з React.

Для всіх зазначених фреймворків характерні такі переваги як: ефективність, гарна швидкість розробки, механізми забезпечення безпеки. Немаловажним є те, що ці JavaScript-фреймворки поширюються безкоштовно. Усі інтерфейсні фреймворки порівняно захищені та дозволяють створювати програмні продукти з розширеним захистом даних. Сьогодні для програмістів стало можливим в режимі реального часу переглядати всі зміни та модифікації у браузері, не боячись втратити статус програми чи сайту, а також без необхідності повторного завантаження сторінок. Більшість фреймворків розробки інтерфейсу пропонують для новачків численні переваги для легкого вивчення. Крім того, технології інтерфейсу мають зручні шари побудови, що робить продукти особливо легкими для масштабування.

На відміну від будь-якої іншої галузі, тенденції розвитку front-end стрімко змінюються, адже front-end стосується того, як виглядатиме цифровий продукт певної компанії і відповідно формує враження користувача про компанію в цифровому світі. Тому з часом змінюються і вдосконалюються і JS-інструменти для ефективного врахування сучасних тенденцій сучасної веброзробки та для задоволення потреб веброзробників. Не існує якогось одного найкращого інтерфейсного фреймворка. Будь-який фреймворк має свою специфіку, свої плюси і мінуси, а вже розробник вибирає той, який якнайкраще відповідатиме потребам відповідного проєкту.

Список використаних джерел:

1. Total number of Websites. URL: https://www.internetlivestats.com/total-number-of-websites/
2. Трофименко О.Г. Сучасний інструментарій веброзробника. *Інформаційне суспільство: проблеми та перспективи* : матер. V всеукр. наук.-практ. конф. (22 травня 2020 р.).
3. Developer Survey 2021. URL: https://insights.stackoverflow.com/survey/2021#technology.
4. Front-end frameworks. The state of JS. URL: https://2021.stateofjs.com/en-US/libraries/front-end-frameworks.
5. GitHub. Vue.js. URL: https://github.com/vuejs/vue
6. Google Trends. URL: https://trends.google.ru/trends/explore?cat=5&date=today%205-y&q=React,%2 Fg%2F11c6w0ddw9,Vue.
7. The State of Developer Ecosystem 2021. URL: https://www.jetbrains.com/lp/devecosystem-2021.
8. GitHub / React. URL: https://github.com/facebook/react.
9. Introducing Hooks, React 16.8. URL: https://reactjs.org/docs/hooks-intro.html
10. GitHub, Angular. URL: https://github.com/angular.

Науковий керівник: доцент Трофименко О. Г.

ДОСЛІДЖЕННЯ РІВНОМІРНОСТІ РОЗПОДІЛЕННЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Мироненко А. А.

студент 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасний розвиток обчислювальної техніки суттєво підвищує значимість використання методів комп'ютерного моделювання у дослідженні процесів управління інфраструктурою підприємств, а також складних технологічних процесів.

Комп'ютерне моделювання ґрунтується на імітації стохастичних процесів з використанням арифметичних датчиків псевдовипадкових чисел (ПВЧ) і відбувається у два етапи: спочатку створюється послідовність рівномірно розподілених на інтервалі [0, 1] випадкових величин, а потім із них формується послідовність, яка відповідає заданому закону розподілення ймовірностей.

Послідовності, сформовані на основі обчислювального алгоритму, циклічно повторюються і, для того щоб вони мали властивості випадкових, період їх повторення має бути якомога більшим. На даний час ця проблема є вирішеною, але, що стосується рівномірності розподілення ймовірностей, то, не зважаючи на заяви розробників, переважна більшість вбудованих у популярні програмні середовища генераторів не відповідає сучасним вимогам [1].

Щоб можна було прийняти рішення по придатність того або іншого генератора псевдовипадкових чисел для моделювання числового потоку з відомим розподіленням ймовірностей, необхідно взяти за основу алгоритм формування рівномірно розподілених чисел, якість якого не нижче, ніж у основного потоку. З урахуванням цього ціллю роботи є розроблення алгоритму для оцінки якості програмних генераторів псевдовипадкових чисел.

Оцінка якості генераторів ПВЧ в програмних середовищах

Сучасні середовища програмування використовують для потреб моделювання лінійний конгруентний генератор (Linear congruent generator LCG) [2], і алгоритм, відомий під назвою Вихор Мерсенна (Mersenne twister, MT), який забезпечує надзвичайно великий період повторення ($2^{19937} - 1$ біт) [3]. Вони обидва входять до складу бібліотек майже всіх відомих спеціалізованих програмних середовищ, призначених для вирішення дослідницьких та інженерних задач.

Найчастіше для перевірки таких датчиків використовують критерій Карла Пірсона χ^2 [3]. Є й інші, більш складні, критерії, але вважається, що якщо перевірка за критерієм χ^2 не дає позитивний результат, то й інші критерії теж не пройдуть.

Суть цього критерію полягає в тому, що спочатку формується досить велика кількість псевдовипадкових чисел розміру N, рівномірно розподілених на інтервалі [0, 1]. Цей інтервал розділяється на однакових підінтервалів. У разі якісного

рівномірного розподілення, очікується, що у кожний інтервал попадає $N_i = N/n$ чисел, як це показано на рисунку 1, а частота попадання числа у той або інший інтервал дорівнює $p_i = 1 / n$.

Рис. 1. Частотна діаграма ідеального генератора ПВЧ

Оскільки в реальній ситуації розподілення чисел на виході генератора відрізняється від рівномірного частоти будуть відрізнятись одна від одної і розподілення буде мати вигляд, наведений на рисунку 2.

Як показано у [3], показник рівномірності $\chi^2_{екс}$, обчислений на основі сформованої генератором ПВП чисел з використанням критерію Пірсона визначається як

$$\chi^2_{екс} = \frac{(N_i - p_i N)^2}{p_i N}. \qquad (1)$$

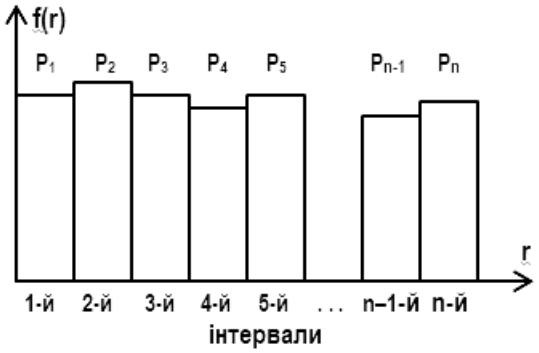


Рис. 2. Частотна діаграма реального генератора ПВЧ

Критичне значення показника $\chi^2_{кр}$ визначається із спеціальних таблиць або обчислюється з урахуванням кількості підінтервалів на яку розбитий інтервал [0, 1] і величина допустимого відхилення від теоретичного значення N/n у процентах.

Для вирішення поставленої задачі було створення програмний продукт, який створює потік псевдовипадкових чисел заданого об'єму, записує його у текстовий файл, а потім переписує його вміст у тимчасовий динамічний масив для подальшого дослідження.

У якості вхідних даних експерименту обрані кількість підінтервалів n = 16, довжина послідовності ПВЧ вище тисячі символів і ступінь відхилення від рівномірності не більше 15%.

Кожне випадкове число, записане у масив, перевіряється окремо на предмет номеру інтервалу у який воно попадає. Одночасно ведеться облік кількості чисел у кожному інтервалі. Отримання цих даних дає можливість обчислення величини $\chi^2_{екс}$, скориставшись виразом (1).

В окремий файл програмного продукту винесена процедура обчислення величини критичного значення $\chi^2_{кр}$. Методику її обчислення можна найти на сайті NIST.

Програмний продукт має графічний інтерфейс, наведений на рисунку 3.

Він дозволяє вводити розмір послідовності N, ступінь відхилення від рівномірності α та ім'я файлу, у якому зберігається сформована послідовності.

На форму проекту у вигляді таблиць виведено дані про вміст файлу з псевдовипадковими числами, кількість випадкових чисел у кожному із 16-ти інтервалів, а також діаграма розподілення ПВЧ в інтервалах. Окремо виводяться дані про змінні $\chi^2_{екс}$ і $\chi^2_{кр}$, а також про очікувану кількість чисел N/n в кожному інтервалі.

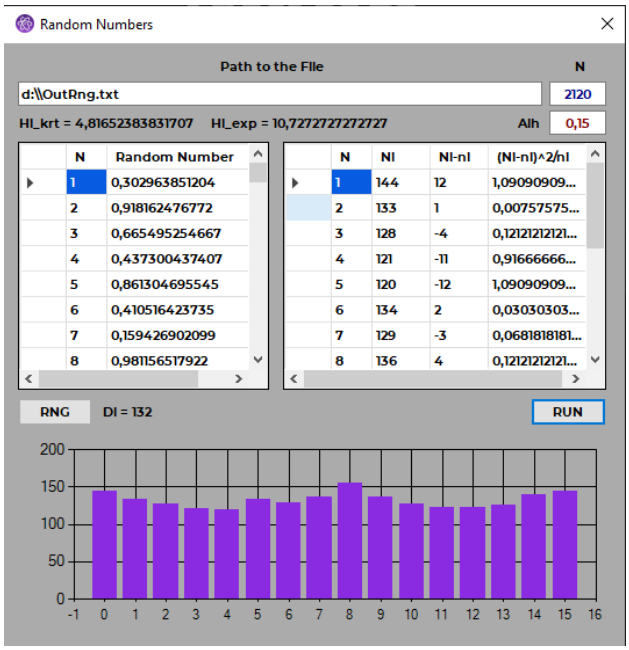


Рис. 3. Зовнішній вигляд графічного інтерфейсу програми

Розроблений програмний продукт дозволяє багаторазово формувати послідовність випадкових чисел, оцінювати кожну з них і порівнювати отриманий показник рівномірності з критичним значенням і, таким чином, накопичувати необхідний статистичний матеріал, на основі якого робиться висновок про придатність даного генератора ПВЧ.

Висновки

Проведені випробування лінійного конгруентного генератора, а також

генератора, побудованого на основі використання чисел Мерсенна, показали, що, не зважаючи на великий період повторення, обидва генератори не забезпечують рівень рівномірності псевдовипадкових чисел на виході алгоритму. При чому, на результати випробувань майже не впливають ні розмір величини сформованої послідовності N, ні обраний показник точності α.

Наведені недоліки не дозволяють використовувати ці генератори для точного моделювання випадкових процесів, які описуються іншими видами законів розподілення випадкових величин. Одною з причин такого явища є те, що арифметичні генератори формують натуральні числа, а вже потім їх перетворюють у дійсні числа шляхом приведення до максимального значення. Саме використання операції ділення дає нерівномірність розподілення вихідних чисел.

Список використаних джерел:

1. Averill M. Law. Simulation modeling and analysis, 5th. ed., McGraw-Hill Education, 2 Penn Plaza, New York, 2015. URL: https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/108-Simulation-Modeling- and-Analysis-Averill-M.-Law-Edisi-5-2014.pdf
2. Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithm, and Source Code in C, 20. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998. doi:10.1002/9781119183471 URL: https://lost-contact.mit.edu/afs/adrake.org/usr/rkh/Books/books/Schneier%20-%20Applied%20Cryptography%202ed%20-%20Wiley.pdf.
3. D. E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998. URL: https://doc.lagout.org/science/0_Computer%20Science/2_Algorithms/The%20Art%20of%20Computer%20Programming%20%28vol.%202_%20Seminumerical%20Algorithms%29%20%283rd%20ed.%29%20%5BKnuth%201997-11-14%5D.pdf

Науковий керівник: доцент Щербина Ю. В.

ВІЗУАЛІЗАЦІЯ АЛГОРИТМУ ДЕЙКСТРИ

Трофименко О. Г.

кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Новіков Д. І.

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сьогодні для ІТ-освіти, і як наслідок для ІТ-галузі, характерні проблеми якості освіти і дефіцит спеціалістів водночас. Здобувачі ІТ-освіти мають багато вчитися і під час навчання, і під час професійної діяльності, щоб встигати за змінами

в ІТ-індустрії загалом та новими трендами у вузькоспеціалізованих напрямках [1].

Нині на співбесідах ІТ-компаній та оцінці кандидатів найму часто питання з алгоритмів рішення задач (Problem Solving) є ключовими. «Алгоритмічні» питання можуть становити від 60% до 100% завдань у співбесіді [2]. Здебільшого такі завдання полягають в неочевидному вирішенні, аніж у реалізації, і дозволяють з'ясувати здатність фахівця до розробки нового функціоналу програмного продукту та оптимізації наявного, що дозволить і надалі просувати компанії вгору.

Тому знання і вміння застосовувати ефективні алгоритми є важливою компетенцією для розробників програмного забезпечення (ПЗ). Алгоритми використовуються практично в усіх сферах інформаційних технологій: в криптографії, при аналізі текстів, зображень і відео, в біоінформатиці, аналізі великих даних, штучному інтелекті, задачах оптимізації тощо.

Переважно основні етапи проектування, розробки та аналізу алгоритмів вивчаються в рамках дисципліни «Алгоритми та структури даних» (АСД) у закладах вищої освіти Україні при підготовці студентів галузі 12 «Інформаційні технології». В університетах світу цей курс здебільшого має назву CS2. Набуті у цьому курсі навички сприятимуть написанню ефективного робочого коду при розробці проектів. Курс АСД (або CS2) є доволі складним для розуміння студентами, багато хто з них сприймає матеріал лише частково [3]. За даними [4], невдачі наприкінці цього курсу складають 5,7%. Серед найскладніших тем курсу дослідники називають алгоритми на графах і деревах, рекурсію, купу, алгоритми сортування та пошуку, аналіз швидкості алгоритмів, зв'язані списки, черги, карти і хеш-таблиці [5-7]. Причому перелік найскладніших тем CS2 суттєво відрізняється у різних дослідників, що може свідчити про наявність суб'єктивних чинників, зокрема: розподіл часу за темами, добір завдань для лабораторних робіт, попередній досвід вивчення програмування у студентів, педагогічна майстерність викладача тощо.

Ефективним підходом до вирішення проблем з опанування студентами складних тем програмного опрацювання графів є допоміжна візуалізація алгоритмів. Адже за даним досліджень [8] мозок людини обробляє зображення в 60 000 разів швидше, ніж текст, і 90% відсотків інформації, що передається мозку, є саме візуальною.

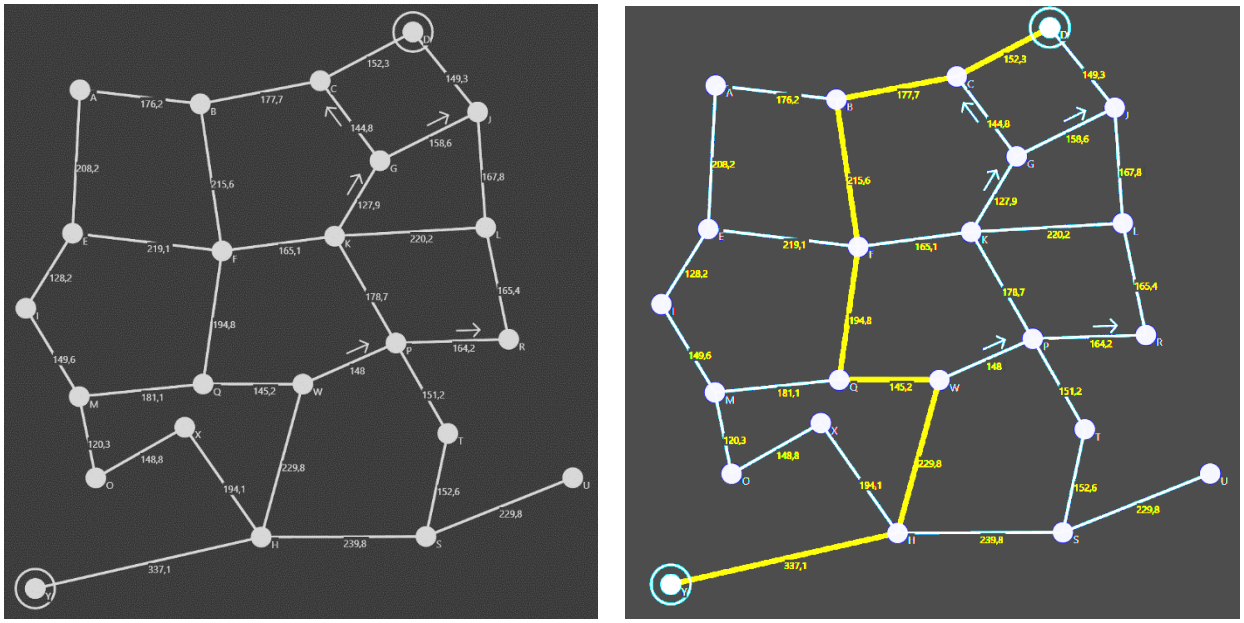
Для програмної реалізації візуалізації алгоритму Дейкстри було використано мову програмування C#, вибір якої зумовлений наявністю в .Net Framework потужних інструментів Windows Forms та Windows Presentation Foundation (WPF) для розробки графічного інтерфейсу користувача (GUI). WPF навіть дозволяє розробляти інтерфейс, побудований на векторній графіці, що дозволяє масштабувати елементи інтерфейсу без втрати якості та без спотворення розмірів.

Розроблений проєкт LOGMAP спрямований на візуальну інтерактивну побудову графів з метою наочної демонстрації ефективної роботи алгоритму Дейкстри для пошуку найкоротшого шляху між двома заданими користувачем

вершинами графа. Користувач може довільно задавати вершини графа на полі, просто клацаючи по ньому у відповідній позиції. Є можливість заповнення поля випадково сформованими вершинами. Поєднувати вершини графа можна у довільно вибраному користувачем порядку. Для економії часу є режим випадкового поєднання вершин графів, що особливо зручно в процесі навчального процесу. Кількість вершин та дуг графів може бути довільною. Можна для кожної вершини задавати назву, наприклад, якогось географічного об'єкта на мапі або назви торгової точки при практичній реалізації графа. Для дуг можна задавати вагу, наприклад, як значення відстані між двома вершинами. Значення ваги для графів може бути комплексною характеристикою, яка враховує декілька чинників, наприклад: відстань, якість дороги, наявність заторів на дорогах тощо. Якщо користувач не задає назви вершин, то вони формуються з усталеного набору, а значення ваги дуг формуються, залежно від відстані між вершинами. Є можливість вимикати відображення значень ваги та назв вершин, якщо не варто захаращувати зайвою деталізацією візуалізацію графа. Закладено можливість задавати односпрямовані дуги для орієнтованих графів, наприклад, якщо це стосується практичного застосування для доріг з односпрямованим рухом.

Окрім зазначених переваг, у проєкті LOGMAP закладено можливість вільної інтерактивної трансформації графа, з можливістю його вільного редагування за допомогою покажчика миші, і навіть масштабування, наприклад для того, щоб детально переглянути та відредагувати якийсь певний фрагмент масштабного графа.

Програмно алгоритм Дейкстри реалізовано в окремому класі з набором відповідних методів та властивостей. Його основний метод GetPath визначає найкоротший шлях поміж точками у формі списку з'єднань вершин графа (рис. 1).

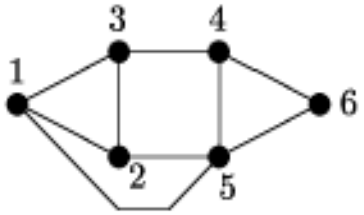


а) *б)*

Рис. 1. Візуалізація алгоритму Дейкстри:
а) задано граф і дві вершини (виділені кільцем) для пошуку найкоротшого шляху;
б) визначено найкоротший шлях між двома заданими вершинами (жовта жирна лінія)

Аргументами цього методу є стартова та кінцева вершини для пошуку найкоротшого шляху поміж ними, а також список усіх вершин графа, які будуть аналізуватися для пошуку шляху від стартової вершини до кінцевої.

У методі GetPath формується словник словників, в якому зберігаються дані з'єднань між вершинами та вага кожного з них. Цей словник можна представити матрицею суміжності (рис. 2). Якщо з'єднання існує, то воно додається до словника.



$$\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Рис. 2. Матриця суміжності графа

При реалізації пошуку ітераційно у циклі за допомогою метода GetSmallest() визначається найближча вершина, оновлюються дистанції до інших вершин методом UpdateDistances(), список невідвіданих вершин сортується, залежно від дистанцій, які зберігаються в словнику, а метод BuildPath() будує шлях у вигляді списку номерів визначених вершин.

Запропонована реалізація алгоритму доволі швидка. Наприклад, пошук найкоротшого шляху на графі на рис. 1 зайняв менше 1 мс. Звісно, що на швидкість пошуку впливають характеристики процесора, кількості вершин та дуг графа. Експериментальні тестові пошуки на графі з 422 вершин і 562 дуг між різними його вершинами показали час в діапазоні від 17 до 24 мс.

Практичне застосування розробленого проєкту LOGMAP під час пояснення роботи алгоритмів на графах у курсі АСД показав гарні показники засвоєння навчального матеріалу, про що свідчать позитивні оцінки успішності шляхом тестування з теми.

Візуалізація складних алгоритмів є сучасним та ефективним підходом для кращого засвоєння їх здобувачами вищої освіти. Важливість курсу АСД в процесі підготовки IT-фахівців змушує викладачів в університетах нашої країни та всього світу приділяти значну увагу вдосконаленню його викладання та шукати нові підходи викладання. Адже розуміння принципів роботи алгоритмів і структур даних під час розроблення програмного забезпечення дозволяє покращити продуктивність програм, поліпшити якість коду і прискорити його роботу, а тому є фундаментальним для становлення майбутніх програмістів.

Список використаних джерел:

1. Прокоп Ю.В., Трофименко О.Г., Задерейко О.В. Аналіз підходів у викладанні початкового курсу програмування в університетах. *Системні технології*. 2021.

№ 4(135). С. 73-84. DOI 10.34185/1562-9945-4-135-2021-08.
2. Прокоп Ю.В., Трофименко О.Г., Дикий О.В. Дослідження підходів до викладання курсу "Алгоритми та структури даних" для студентів ІТ-спеціальностей. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. Серія «Технічні науки». 2021. Том 32 (71) Ч. 1 № 2. С. 216-220. DOI: 10.32838/2663-5941/2021.2-1/34.
3. Yeomans L., Zschaler S., Coate K. Transformative and Troublesome? Students' and Professional Programmers' Perspectives on Difficult Concepts in Programming. *ACM Transactions on Computing Education*. Vol. 1, No. 1. P. 1-27. DOI: 10.1145/3283071.
4. Layman L., Song Y., Guinn C. Toward Predicting Success and Failure in CS2: A Mixed-Method Analysis. *ACM Southeast Conference* (ACM SE '20). New York, NY, USA, 2020. P. 218-225. DOI: 10.1145/3374135.3385277.
5. Wittie L., Kurdia A., Peng J., Kelly J., Huggard M. Developing a Concept Inventory for Computer Science 2: What should it focus on and what makes it challenging? IEEE Frontiers in Education Conference (FIE'20). 2020. P. 1-8. URL: http://www.tara.tcd.ie/bitstream/handle/2262/92988/CS2_Concept_Inventory_FIE_2020.pdf;jsessionid=BD4D1BE6611256FB0C6A3CF76556F59C?sequence=1.
6. Zingaro D., Taylor C., Porter L., Clancy M., Lee C., Nam L., Webb K. Identifying student difficulties with basic data structures. In Proceedings of the 14th ACM Conference on International Computing Education Research. 2018. P.169-177. URL: https://www.cs.oberlin.edu/ ~ctaylor/pubs/icer143-zingaroA.pdf
7. Tenenberg J., Murphy L. Knowing what I know: An investigation of undergraduate knowledge and self-knowledge of data structures. Computer Science Education. 2005. Vol. 15, No. 4. P. 297-315. DOI: 10.1080/08993400500307677
8. Humans Process Visual Data Better. URL: https://www.t-sciences.com/news/humans-process-visual-data-better

ВИКОРИСТАННЯ КОМПЛЕКСНИХ КВАДРАТИЧНИХ СПЛАЙНІВ В ЗАДАЧАХ LBS-ПОЗИЦІОНУВАННЯ

Стрелковська І.В.

доктор технічних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Соловська І.М.

кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Стрімкий технологічний розвиток інфокомунікаційних мереж зумовлює впровадження множини застосунків та сервісів, які використовують поточне LBS (Location-based Services) місцезнаходження користувача в реальному часі й краудсорсінг (Crowdsourcing), що потребує постійного вдосконалення методів позиціонування з метою підвищення точності місцезнаходження. Особливої уваги заслуговують задачі LBS-позиціонування користувачів Indoor всередині

приміщень в умовах високої концентрації користувачів та наявності складнощів при поширенні радіосигналів [1-8]. Відомі методи LBS-позиціонування Indoor базуються на отриманих значеннях відстані між джерелом та приймачем сигналу з використанням наступних методів: RSS (Received Signal Strength) на базі визначення відстані вимірювання рівня потужності приймаємого сигналу, AOA (Angle of Arrival) – на вимірі кута надходження сигналу щодо джерела, TOA (Time of Arrival) та TDoA (Time Difference of Arrival) – на вимірюванні часу затримки поширення радіосигналу [1-3]. Позиціонування користувача відбувається за допомогою низки методів: тріангуляції або трилатерації [1-4], Fingerprinting [4] або ймовірносних методів [5], методу *k*-найближчих сусідів *k*-NN (*k*-Nearest Neighbor) та зваженого метода *k*-найближчих сусідів з використанням вагових коефіцієнтів *k*-WNN (*k*-Weighted Nearest Neighbor) [1-4], байєсівського методу [6] та нейронних мереж [7]. Кожен з вищенаведених методів має низку переваг та недоліків, але всі ці методи показують значні похибки при позиціонуванні в приміщенні. Очевидно, що для вирішення поставленої задачі доцільно здійснити пошук математичного методу, альтернативного до відомих раніше, який дозволить значно спростити процес рішення та одночасно надати нові можливості рішення. Таким рішенням можуть бути методи інтерполяції, апроксимації та екстраполяції за допомогою дійсних та комплексних сплайн-функцій [8]. Раніше авторами в роботах [9-10] при вирішенні задач відновлення та оцінки станів даних, сигналів та трафіку, задач обробки сигналів та підвищення характеристик якості QoS/QoE при функціонуванні інфокомунікаційних мереж та прогнозування характеристик трафіку різних застосунків були використані дійсні сплайн-функції (лінійні , квадратичні, кубічні, B-сплайни), які спростили вирішення багатьох завдань. В роботах [11-14] авторами вирішено завдання позиціонування користувача в мережі Indoor за допомогою комплексних плоских сплайнів. Розглянемо використання комплексних плоских квадратичних сплайнів для рішення завдань LBS-позиціонування користувача в мережі Indoor.

Метою даної роботи є рішення завдання LBS-позиціонування в мережі Indoor на базі комплексних плоских квадратичних сплайнів для підвищення точності визначення місцезнаходження користувача.

Розглянемо мережу Indoor в приміщенні, яку показано на рис. 1. Вважаємо, що мережа Indoor складається зі сукупності точок доступу AP_i, де i – кількість точок доступу AP_i, причому $i=\overline{1,3}$, $AP_i\ (x, y)$ – координати i-тої точки доступу AP_i. Тоді точки доступу AP мають наступні координати: $AP_1\ (x_1, y_1)$, $AP_2\ (x_2, y_2)$, $AP_3\ (x_3, y_3)$, координати користувача $M\ (x, y)$. Вважаємо, що в кожній точці розглядаємої мережі Indoor пристрій користувача знаходиться в радіусі дії не менш ніж трьох точок доступу AP_i. Знайдемо координати користувача $M\ (x, y)$, використовуючи модифікований метод позиціонування користувача в мережі Indoor на

основі методу Fingerprinting з використанням комплексних плоских сплайнів, запропонований в роботах [11-14].

Алгоритм LBS-позиціонування користувача (рис. 1) в мережі Indoor розглянемо на основі методу Fingerprinting та комплексних плоских сплайнів [11-14]. На першому етапі алгоритму виконується формування бази даних Fingerprinting DataBase, яка зберігає значення виміряних потужностей RSSI (Received Signal Strength Indicator) точок доступу APi, $i=\overline{1,3}$ у заздалегідь заданих точках приміщення RP (Reference Point) та дані MAC-адрес усіх точок доступу AP_i, $i=\overline{1,3}$ ($MAC_{1,1}$, $RSSI_{1,1}$), ($MAC_{1,2}$, $RSSI_{1,2}$), ($MAC_{1,3}$, $RSSI_{1,3}$) [11-14].

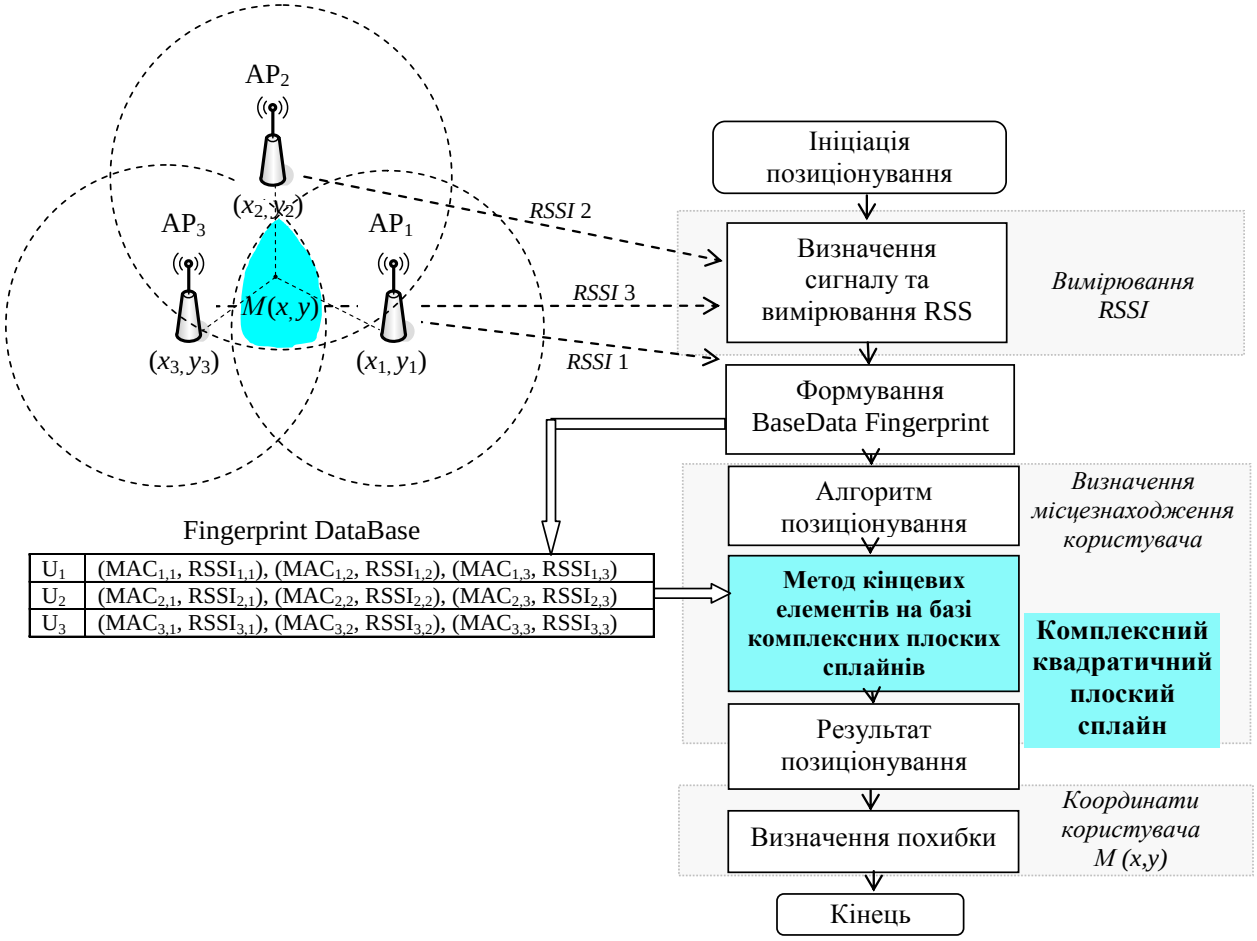


Рис. 1. Алгоритм LBS-позиціонування користувача на основі методу Fingerprinting з використанням комплексних плоских сплайнів

Позиціонування пристрою користувача відбувається до найближчих точок доступу AP_i, $i=\overline{1,3}$, у відповідності до якого кожна точка доступа AP_i, виконує вимірювання значення потужності сигнала RSSI та порівнює отримані значення з даними Fingerprint DataBase. Визначення координат місцезнаходження виконується шляхом побудови квадратичного плоского сплайна. Для знаходження похибки позиціонування використовується Лемма.

Процес побудови комплексних плоских сплайнів приведений в роботах [11-14]. Нехай область $\overline{G} \subset Q$, де $\overline{G} = G \bigcup \partial G$, ∂G – границя області G, $Q = [a, a+H] \times [b, b+H]$ – квадрат зі стороною $H > 0$ (рис. 2), N – натуральне число, $h_N = \frac{H}{N}$, $x_k = a + kh_N$, $y_j = b + jh_N$, $k, j = 0, 1, \ldots, N$. Область $Q = \bigcup_{k,j=0}^{N-1} Q_{k,j}$ складається з Q_{kj} – квадратних клітин з кроком h_N, тоді $Q_{k,j} = \left\{ z = x + iy : x \in [x_k, x_{k+1}] \ , y \in [y_j, x_{j+1}] \right\}$.

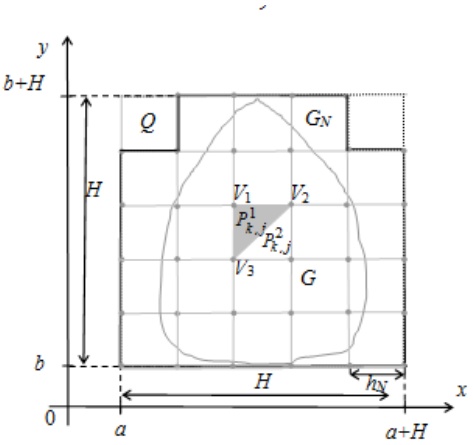


Рис. 2. Побудова клітинної області G

Таке розбиття позначимо через Δ_N.

Визначимо область G_N як об'єднання усіх квадратних клітин $Q_{k,j}$, для яких $Q_{k,j} \cap G \neq \varnothing$. Кожен квадрат $Q_{k,j} \subset G_N$ розіб'ємо діагоналлю на два трикутники $P^1_{k,j}$ та $P^2_{k,j}$. Таке розбиття позначимо Δ'_N. Індекс N в позначеннях h_N, Δ_N, Δ_N' будемо опускати, якщо розглядається фіксоване розбиття. Позначимо через G'_N – об'єднання всіх трикутників $P^1_{k,j}$ та $P^2_{k,j}$, для яких $P^1_{k,j} \cap G \neq \varnothing$, $P^2_{k,j} \cap G \neq \varnothing$. Розглянемо один з трикутників $P^1_{k,j}$, $P^2_{k,j}$, який входить до області G'_N з вершинами V_1, V_2, V_3 такими, що виконуються вимоги: Im V_1 = Im V_2, Re V_2 = Re V_3.

Відповідно [11-14], побудуємо по області G_N комплексний плоский квадратичний сплайн $S_\Delta(z)$, який інтерполює функцію $f(z)$ у вершинах квадратів $Q_{k,j}$, які увійшли до G_N:

$$S_\Delta(z) = a + bz + c\bar{z} + d(z^2 - \bar{z}^2), \qquad (1)$$

при $z \in Q_{k,j} \subset G_N$, де коефіцієнти a, b, c, d визначаються з інтерполяційних умов в точках $z_{k,j} = x_k + iy_j$:

$$S_\Delta(z_{k,j}) = f(z_{k,j}), \quad S_\Delta(z_{k+1,j}) = f(z_{k+1,j}),$$
$$S_\Delta(z_{k,j+1}) = f(z_{k,j+1}), \ S_\Delta(z_{k+1,j+1}) = f(z_{k+1,j+1}).$$

Функція $S_\Delta(z)$ – неперервна в області G_N [11-14].

<u>Лемма.</u> Нехай функція $\varphi(z)$ неперервна в області $\overline{G_N}$, а $S_\Delta(z)$ – комплексний плоский квадратичний сплайн вигляду (1), який інтерполює функцію $f(z)$ у вузлах $\{z_{kj}\}$, тоді

$$\left| f(z) - S_\Delta(z) \right| \le 4\omega(f, h),$$

де $h = h_N$ та $\omega(f, h)$ – модуль неперервності функції f в G'_N,

$$\left| f(z) - S_\Delta(z) \right| \prec h\omega(f, h),$$

де символ $\prec$ у виразі $a \prec cb$ визначає, що для $a > 0$ та $b > 0$ виконується нерівність $a \leq cb$, де c – const.

Висновки

1. Розглянуто задачу позиціонування користувача для мережі Indoor в приміщенні та методи, які використовуються для визначення LBS-місцезнаходження користувачів всередині приміщень.

2. Запропоновано використання комплексної сплайн-апроксимації на базі комплексних квадратичних плоских сплайнів в методі Fingerprinting для підвищення точності позиціонування.

3. Встановлено, що використання сукупності методів Fingerprinting та комплексної сплайн-апроксимації при позиціонуванні користувача в мережі Indoor дозволяє підвищити точність позиціонування і досягти зниження обчислювальної складності процесу, що забезпечить значне скорочення часу позиціонування.

Список використаних джерел:

1. Hameedah S.H. et al., «An Overview of Local Positioning System: Technologies, Techniques and Applications,» International Journal of Engineering & Technology, vol. 7(3), pp. 1-5, 2018. https://doi.org/10.14419/ijet.v7i3.25.17459.
2. F. Gu et al., «Indoor Localization Improved by Spatial Context – A Survey,» ACM Computing Surveys, vol. 52(3):64, pp. 1-35, 2019, https://doi.org/10.1145/3322241.
3. G. Li, E. Geng, Z. Ye, H. Zhu, «An Indoor Positioning Algorithm Based on RSSI Real-time Correction,» in 14th IEEE International Conference on Signal Processing (ICSP), 2018, https://doi.org/10.1109/ICSP.2018.8652382
4. A.P. Rahmadini, P. Kristalina, A. Sudarsono, «Optimization of Fingerprint Indoor Localization System for Multiple, Object Tracking Based on Iterated Weighting Constant – KNN Method», International Journal on Advanced Science Engineering Informational Technology, vol. 8(3), pp. 998-1007, 2018, https://doi.org/10.18517/ijaseit.8.3.6086.
5. P. Bráulio H.O.U.V., Horácio A.B.F. de Oliveira, and E. J.P. Souto, "Factor Optimization for the Design of Indoor Positioning Systems Using a Probability-Based Algorithm," Journal of Sensor and Actuator Networks, *vol. 10*, no. 1:16, 2021. https://doi.org/10.3390/jsan10010016.
6. Q. Yang, S. Zheng and M. Liu, Research on Wi-Fi indoor positioning in a smart exhibition hall based on received signal strength indication, Wireless Com Network, 2019. https://doi.org/10.1186/s13638-019-1601-3.
7. H. Mehmood, N.K. Tripathi, T. Tipdecho, «Indoor Positioning System Using Artificial Neural Network,» Journal of Computer Science, vol. 6 (10), pp. 1206-1212, 2010. https://doi.org/10.3844/jcssp.2010.1219.1225.
8. Strelkovskaya I., Solovskaya I., Strelkovska J. Spline-approximation and spline-extrapolation methods in telecommunication problems. In: Ilchenko M., Strelkovska I. (eds) Current Trends in Communication and Information Technologies. Lecture Notes in Networks and Systems, vol. 212, pp. 3-20. Springer, Chap № 1. https://doi.org/10.1007/978-3-030-76343-5_1.

9. Strelkovskaya I., Solovskaya I., Makoganiuk A. Different extrapolation methods in Problems of Forecasting. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham, pp. 217-228. https://doi.org/10.1007/978-3-030-58359-0_12
10. Strelkovskaya I., Solovskaya I. Using spline-extrapolation in the research of self-similar traffic characteristics. Journal of Electrical Engineering. Vol. 70 (2019), Is. 4, pp. 310-316. https://doi.org/10.2478/jee-2019–0061
11. Strelkovskaya I., Solovskaya I., Strelkovska J. «The use of linear complex planar splines to improve the accuracy of determining the location of the user in Wi-Fi/Indoor networks,» in 2021 International Scientific-Practical Conference Proceedings (PICS&T), 2021, pp. 1-5.
12. Strelkovskaya, I. Solovskaya I., J. Strelkovska, «Linear complex planar splines in Wi-Fi/Indoor positioning problems,» in 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (IEEE UkrMiCo), 2021, pp. 84-87. https://doi.org/10.1109/UkrMiCo52950.2021.9716612
13. Strelkovskaya I., Solovskaya I., Strelkovska J., «Fingerprinting/Indoor positioning using complex planar splines», in Journal of Electrical Engineering, vol. 72, №6, 2021, pp. 401-406. https://doi.org/10.2478/jee-2021-0057.
14. Strelkovskaya I., Solovskaya I., Strelkovska J., Grigoryeva T., «Using quadratic complex planar splines in solving local positioning problems,» in IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2022, pp.1-4.

ВИКОРИСТАННЯ СПЛАЙН-АПРОКСИМАЦІЇ ТА СПЛАЙН-ЕКСТРАПОЛЯЦІЇ В ЗАДАЧАХ ІНФОКОМУНІКАЦІЙ

Стрелковська І.В.

доктор технічних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Соловська І.М.

кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Розвиток мереж Future Networks зумовлює стрімку зміну технологій, оновлення протоколів та вдосконалення механізмів підтримки необхідних характеристик якості QoS/QoE (Quality of Service/ Quality of Experience) [1]. Такі зміни потребують кардинального перегляду відомих рішень та пошуку нових методів рішення задач аналізу та синтезу інфокомунікацій. В залежності від характеру розглядаємих задач отримання результатів можливе за допомогою оцінок інтерполяції, екстраполяції та апроксимації, адже ефективність рішення задач аналізу

та синтезу інфокомунікаційних мереж безпосередньо залежить від точності отриманих результатів.

Метою даної роботи є пошук нових методів рішення задач аналізу та синтезу в інфокомунікаціях для підвищення характеристик якості функціонування інфокомунікаційних систем.

На практиці при рішенні задач аналізу та синтезу інфокомунікаційних мереж та систем, знайшла своє використання сплайн-апроксимація з використанням різних сплайн-функцій (лінійних, квадратичних та кубічних), результати якої дозволяють вирішувати значний клас задач [2-5]:

- відновлення випадкових сигналів й самоподібного трафіка, рішення яких дозволяють отримати необхідні значення між вузлами інтерполяції з необхідною похибкою [3];
- відновлення станів мережних об'єктів та характеристик в реальному часі, рішення яких забезпечить отримання рекурсивних оцінок стану часу затримки протоколу RTP/RTCP, ємності завантаження буфера RED та інших з метою зменшення похибки відновлення [4];
- управління мережними об'єктами і мережею в цілому, які базуються на результатах моніторингу та обробці отриманих даних [5];
- підтримки процедур функціонування об'єктів і мережі в цілому з метою підвищення характеристик якості QoS/QoE функціонування [3].

Використання сплайн-апроксимації дозволило отримати рішення задачі апроксимації спектральної характеристики сигналу [6]:

$$|G(j\omega)| = \begin{cases} UT, & |\omega| < \omega_A, \\ G_{\Delta 1}(\omega), & \omega_A \le |\omega| \le \omega_C, \\ G_{\Delta 2}(\omega), & \omega_C < |\omega| \le \omega_B, \\ 0, & \omega_B < |\omega|, \end{cases}, \qquad (1)$$

де $U = g(0)$, $\omega_A = (1-\alpha)\omega_C$, $\omega_B = (1+\alpha)\omega_C$, $\omega_C = \pi/T$ $\alpha = (\omega_C - \omega_A)/\omega_C =$

$= (\omega_B - \omega_C)/\omega_C$ – коефіцієнт скруглення спектральної щільності $(0 \le \alpha \le 1)$, який визначає ширину перехідної області $[\omega_A, \omega_B]$, $2\Delta\omega = 2\alpha\omega_C$ – ширина перехідної області, $\alpha = \Delta\omega/\omega_C$.

З урахуванням непарної симетрії спектральної щільності сигнала (1) відносно точки *C*, функції $G_{\Delta 1}(\omega)$ та $G_{\Delta 2}(\omega)$ пов'язані рівняннями [6]

$$G_{\Delta 1}(\omega) = UT - G_{\Delta 2}(2\omega_C - \omega), \quad \omega_A \le |\omega| \le \omega_C, \qquad (2)$$

$$G_{\Delta 2}(\omega) = y(\omega) = a + b(\omega - \omega_C) + c(\omega - \omega_C)^2 + d(\omega - \omega_C)^3, \quad \omega_C \le \omega \le \omega_B,$$

де *a, b, c, d* знаходяться з умов інтерполяції виду (3)

$$\begin{cases} y(\omega_C) = a = y_C; \\ y(\omega_B) = a + b\Delta\omega + c\Delta\omega^2 + d\Delta\omega^3 = y_B; \\ y'(\omega_C) = b = y'_C; \\ y'(\omega_B) = b + 2c\Delta\omega + 3d\Delta\omega^2 = y'_B. \end{cases} \quad (3)$$

Сплайн-апроксимація сигналу *f*(*x*) кубічним сплайном (рис. 1).

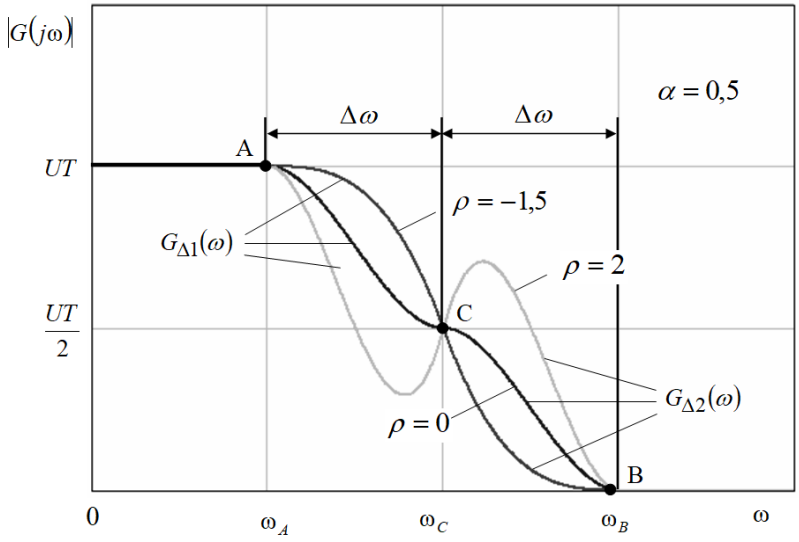


Рис. 1. Сплайн-інтерполяція спектра сигналу *f*(*x*) кубічним сплайном

Сплайн-апроксимація спектральної характеристики в перехідній області дає змогу описувати кубічний сплайн, забезпечуючи необхідну гладкість функції та синтез сигналу, що практично призводить до швидкого затухання сигнальної функції та концентрації енергії в окремих пелюстках [6].

На сучасному етапі розвитку інфокомунікацій важливим питанням є вирішення задач прогнозування характеристик основних параметрів мереж і систем, яка дозволяє отримати необхідні результати з найменшими обчислювальними ресурсами та затратами часу. Розглянемо сплайн-екстраполяцію (на базі лінійних, квадратичних та кубічних слайнів) на прикладі самоподібного трафіку, коли необхідно прогнозувати характеристики трафіку зовні відрізку [*a;b*] [7-10]. Нехай, для визначеності, це буде точка x_c, $x_c > x_N = b$, $x_c - b = h$, де h – крок розбиття відрізку [*a;b*], $h = \dfrac{b-a}{N}$.

Розглянемо два варіанти екстраполяції самоподібного трафіку (рис. 2 та рис. 3).

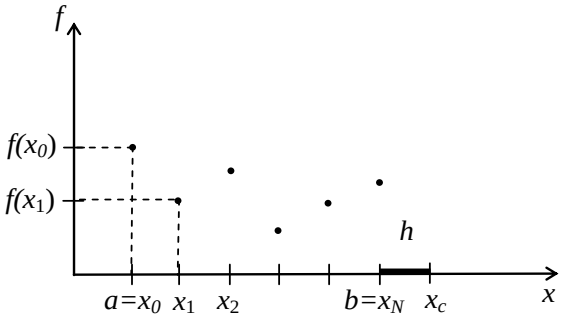


Рис. 2. Екстраполяція самоподібного трафіка на відрізку $[b;x_c]$ за умови $f(x_c) = f(x_1)$

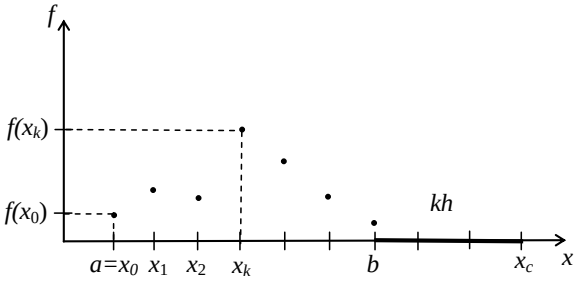


Рис. 3. Екстраполяції самоподібного трафіка на відрізку $[b;x_c]$ за умови $f(x_{kh}) = f(x_c)$

В першому випадку покладемо, що $f(x_c) = f(x_1)$ та побудуємо сплайн-функцію на відрізку $[b;x_c]$ (рис. 2). В другому випадку (рис. 3) покладемо $f(x_k) = f(x_c)$, де $x_k = x_0 + kh$, де k – натуральне. якщо $kh \neq x_c - b$, то в якості $f(x_c)$ беремо значення функції $f(x)$, яке найближче до точки x_k [7-10].

Результати екстраполяції самоподібного відеотрафіку показано на рис. 4.

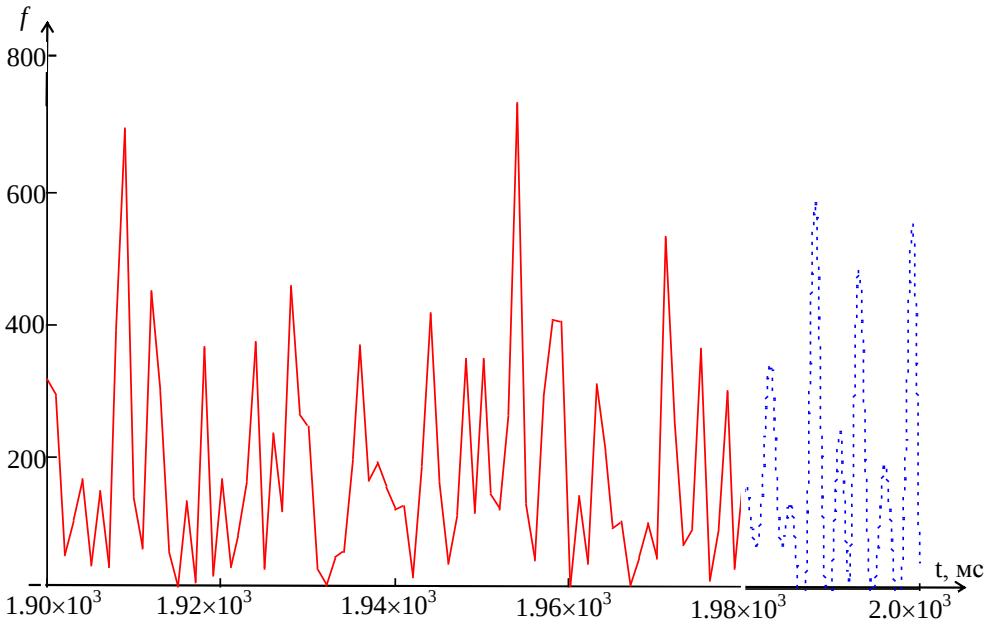


Рис. 4. Відеотрафік, отриманий за допомогою Open Source ресурсу Net Flow Analyzer, який розглядається на відрізку [1900;1980] мс (*червона лінія*) та його екстраполяція кубічним сплайном на відрізку [1980;2000] (*синя пунктирна лінія*)

Використання сплайн-екстраполяції дозволило вирішити значний клас задач аналізу та синтезу інфокомунікацій [7-11]:

- прогнозування характеристик трафіку мережних об’єктів, рішення яких в реальному часі для різних видів трафіку (data traffic, voice traffic, telemetry traffic та video streaming traffic) забезпечить можливості підтримки характеристик якості QoS/QoE [7-11];

- підтримки характеристик якості QoS/QoE, а, саме, характеристик часу затримки та ймовірності втрат й спотворення пакетів при обслуговуванні різних видів трафіку та формуванні вимог до мережних буферних пристроїв [9];
- вибору оптимальної конфігурації об'єктів мережі, рішення яких базується на результатах прогнозування характеристик трафіку об'єктів і мережі в цілому для підвищення характеристик якості функціонування інфокомунікаційної мережі [11].

Висновки

1. Розглянуто низку задач аналізу та синтезу, які потребують рішення в інфокомунікаціях та пошуку ефективних математичних методів, які дозволять спростити процес рішення та одночасно отримати рішення.

2. Запропоновано використання сплайн-апроксимації, яка дозволяє значно простіше отримати рішення класу задач, таких як, відновлення та оцінки станів (даних, сигналів, трафіка), задач обробки сигналів та зображень, включно з задачами фільтрації та стиснення даних, виявлення та вимірювання сигналів та підвищення характеристик якості QoS функціонування інфокомунікаційних мереж з необхідною похибкою.

3. Використано метод сплайн-екстраполяції на базі різних сплайн-функцій (лінійних, квадратичних, квадратичних B-сплайнів, кубічних, кубічних B-сплайнів та кубічних сплайнів Ерміта), який дозволяє отримати рішення задач прогнозування характеристик трафіку та підвищити точність прогнозу, забезпечивши його масштабованість та використання для різних застосунків.

Список використаних джерел:

1. Donovan J. Building the Network of the Future: Getting Smarter, Faster, and More Flexible with a Software Centric Approach. Donovan John, Prabhu Krish (eds.). Chapman and Hall/CRC, 2017.
2. Strelkovskaya I., Solovskaya I., Strelkovska J., «Spline-Approximation and Spline-Extrapolation Methods in Telecommunication Problems», Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems, vol 212, Springer, Cham, 2021, P. 3-22. URL: https://doi.org/10.1007/978-3-030-76343-5_1.
3. Strelkovskaya I.V., Bukhan D.Yu., «Restoration of continuous signals based on the Kalman-Bucy filter and cubic splines», Radio engineering: All-Ukr. Inter. scien. tech. col., Vol. 156, P. 61-63.
4. Strelkovskaya I., Solovskaya I., Severin N., Paskalenko S., «Spline approximation based restoration for self-similar traffic», Eastern-European Journal of Enterprise Technologies, 3/4 (87), P. 45-50. URL: https://doi.org/10.15587/1729-4061.2017.102999.
5. Стрелковская И.В., Лысюк Е.В., Золотухин Р.В. «Восточно-Европейский журнал передовых технологий», Т.2, № 9(62), С. 12-15 URL: https://doi.org/10.15587/1729-4061.2013.12437.

6. Strelkovskaya I., Solovskaya I., Makoganiuk A. A Study of the Extremum of the Total Energy of the Selective Signals Constructed by Quadratic Splines. Periodica Polytechnica Electrical Engineering and Computer Science. 2019, 63(1), pp. 30-36. URL: https://doi.org/10.3311/PPee.12457
7. Strelkovskaya I., Solovskaya I., «Using spline-extrapolation in the research of self-similar traffic characteristics», *Journal of Electrical Engineering*, Vol. 70, Is. 4, P. 310-316. URL: https://doi.org/10.2478/jee-2019–0061.
8. Strelkovskaya I., Solovskaya I., Makoganiuk A., «Different extrapolation methods in Problems of Forecasting», Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-58359-0_12.
9. Стрелковська І.В. Прогнозування характеристик самоподібного трафіку за допомогою сплайн-екстраполяції / І.В. Стрелковська, І.М. Соловська, Макоганюк А.О., Северин М.В. // *Вісник університету «Україна»*. 2019. № 1 (22). С. 87-94.
10. Strelkovskaya I. Use of spline-extrapolation to increase the quality indicators of telecommunication systems / I. Strelkovskaya, I. Solovskaya, V. Tolmak // *Збірник наукових праць ОНАЗ ім. О.С. Попова*. 2019. Вип. 2. С. 77-85.
11. Поповский В.В. Точность процедур фильтрации, экстраполяции и интерполяции случайных проессов / В.В. Поповский, И.В. Стрелковская // *Проблеми телекомунікацій*. 2011. № 1(3). С. 3-10.

РОЗРОБКА НОВИННОГО ТЕЛЕГРАМ-БОТА

Тітієвський В. О.

студент 2-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В наш час інтернет став невід'ємною частиною кожної людини. За допомогою всесвітньої мережі люди працюють, навчаються і спілкуються через різноманітні соціальні мережі, навіть не виходячи зі своїх домівок. Так, лише за період з 2020 по 2021 рік українська аудиторія соцмереж зросла на 7 мільйонів [1].

Телеграм – один з найпопулярніших месенджерів у світі. Кількість його користувачів перевищує 550 млн [2]. Вагомою перевагою Телеграма є гарна підтримка телеграм-ботів, причому функціонал наявних ботів вражаючий: одні – націлені на інформування потенційних клієнтів, другі – орієнтовані на продаж, треті – діють виключно як особисті помічники. Чат-боти використовуються в таких областях, як: сервіси електронної комерції, кол-центри, ігрова індустрія. Все залежить від функціонала, закладеного в програму [3].

Особливо популярними та затребуваними за умов початку карантину через COVID-19, а тепер за умов війни стали новинні чат-боти як зручні та швидкі сервіси інформування відповідних підписників. В цей нелегкий час новинні телеграм-боти повсюдно використовують і на персональних комп'ютерах, і на мобільних телефонах для вчасного отримання важливих новин.

Для розробки такого роду чат-ботів зручно використовувати програмні засоби інтерпретованої об'єктно-орієнтованої мови Python. Це мова програмування високого рівня зі строгою динамічною типізацією [4], яка поєднує численні переваги [5]: гнучкість, швидкість, ефективність, надійність та наявність потужних фреймворків і бібліотек, серед яких є бібліотеки для створення телеграм-ботів.

Специфіка новинного, пропонованого у роботі телеграм-бота полягає в тому, що він не постійно відправляє численні новини, а тільки за бажанням користувача при натисканні відповідної кнопки, щоб не відволікати і не дратувати користувача. Отже, роботу такого бота не потрібно припиняти або вимикати прийом нав'язливих, недоречних або невчасних повідомлень.

Для створення такого роду бота потрібне долучення таких бібліотек:

- *requests* – для відправки HTTP-запитів;
- *emoji* – для додавання емодзі до повідомлень та кнопок;
- *json* – для кодування та декодування даних у зручному форматі;
- *bs4* – для вилучення даних з файлів HTML та XML;
- *aiogram* – повністю асинхронна бібліотека для Telegram Bot API допоможе зробити бота простим та швидким.

Джерелом новин використовуються лише офіційні українські новинні портали [5]. Телеграм-бот має декілька функцій, однією з яких є отримання останніх новин з сайту за допомогою бібліотеки bs4 та запис цієї інформації до json-файлу. У боті також є кнопка, яка формує набори з 10-ти новин в ряд. Зручною функцією розробленого чат-бота є кнопка «Мапа», за допомогою якої можна перейти на сайт з мапою воєнних дій в Україні, що часто оновлюється.

За допомогою представленого новинного бота можна з легкістю, в будь-який зручний для підписника час почитати останні новини своєї держави у вибраному форматі поінформування. Можна скористатись вбудованою мапою, щоб проаналізувати ситуацію на фронтах України. За нинішніх умов розробка такого роду чат-боту є вельми актуальною, а сам чат-бот — затребуваним у користувачів. Після закінчення війни цей бот можна використовувати для подорожей та отримання вже мирних новин про відбудову нашої країни.

Список використаних джерел:

1. За рік кількість українців у соцмережах зросла на 7 мільйонів – дослідження. URL: https://www.epravda.com.ua/news/2021/03/17/672023/
2. Телеграм в цифрах: в каких странах работает мессенджер и как переживает блокировки. URL: https://daily.afisha.ru/infoporn/22599-telegram-v-cifrah-v-kakih-stranah-rabotaet-messendzher-i-kak-perezhivaet-blokiriovki/
3. Трофименко О.Г., Прокоп Ю.В., Задерейко О.В., Логінова Н.І. Класифікація чат-ботів. *Системні технології*. 2022. № 2 (139). С. 147-159. DOI: 10.34185/1562-9945-2-139-2022-14. URL: https://journals.nmetau.edu.ua/index.php/st/issue/view/120/87.
4. Python. URL: https://uk.wikipedia.org/wiki/Python

5. Top 10 reasons why Python is so popular with developers in 2022. URL: https://www.upgrad.com/blog/reasons-why-python-popular-with-developers/#1_Easy_to_Learn_and_Use
6. Новини. URL: https://zaxid.net/news/

Науковий керівник: доцент Трофименко О.Г.

ДЕЯКІ АСПЕКТИ МЕТОДИКИ ВИКЛАДАННЯ КУРСУ «ВЕБТЕХНОЛОГІЇ ТА ВЕБДИЗАЙН» ДЛЯ СТУДЕНТІВ ІТ-ГАЛУЗІ

Толокнов А. А.

асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Мета вивчення дисципліни: формування теоретичних знань та професійних практичних навиків проектування, макетування та редагування веборієнтованих інформаційних продуктів, підготувати майбутнього фахівця до роботи в онлайн-середовищі, із сайтами компаній та власними сайтами.

У дисципліні вивчаються новітні вебтехнології через призму вебдизайну. Вебдизайн – це розділ дизайну, що стосується конструювання вебресурсів і поєднує елементи художніх, технологічних, комерційних та інформаційних наук. Термін складається з двох частин: «веб» – скорочена назва Всесвітньої павутини та «дизайн» – слово, яке означає проектування, конструювання, планування, креслення, малювання, процес створення нових предметів так, щоб їхня форма відповідала змісту. Отже, термін «вебдизайн» означає проектування для інтернету [1].

Дисципліна в основному присвячена front-end розробці в тій її частині, яка зосереджена на макетуванні, верстці, створення інтерфейсу користувача, ергономіці, юзабіліті, доступності, адаптивності тощо. Вивчаються такі нові концепції для макетування розкладок вебсторінок, як flex і grid. Для прискорення front-end розробки використовуються фреймворки. В даному випадку для макетування і верстки вивчається доволі популярний фреймворк Bootstrap.

Завдяки тому, що в CSS3, з'явилися нові можливості: плавні переходи, анімація, фільтри, трансформації, градієнти тощо, це дало змогу не робити ці ефекти, як раніше, за допомогою JavaScript. Тому вивчаються лише елементи мови програмування JavaScript. Більш детально мови програмування для веббудування розглядаються на наступному курсі – «Вебпрограмування» [2]. В контексті будування повноцінного сайту вивчається система управління контентом (CMS) Wordpress, яка, завдяки використанню різноманітних плагінів, дозволяє створити мабуть будь-який сайт, без знання серверної мови програмування.

Для навчання front-end розробки використовують «прості» редактори, такі як: Sublime Text, Atom, Brackets, Notepad ++, Visual Studio Code (VSCode) та інші.

В цьому курсі ми рекомендуємо використовувати безкоштовний кросплатформовий редактор з відкритим вихідним кодом від фірми Microsoft – Visual Studio Code (https://code.visualstudio.com/). Створювати теки й файли можна прямо з редактора. Для прискорення написання коду використовується розширення Emmet, яке необхідно встановлювати у інші редактори. Для VSCode це розширення вже присутнє після встановлення редактора.

Далі перелічені рекомендовані розширення для VSCode: Auto Rename Tag, EasyZoom, htmltagwrap, Indent one space, Insert
 Tag, open in browser тощо. Кількість розширень можна варіювати і збільшувати, перетворюючи редактор на серйозний IDE. Окремо зупинимося на розширеннях Live Server Preview і Live Server. Live Server Preview ділить вікно редактора навпіл. Одна частина редактора використовується для написання коду, а друга – «в живу» відображає результат виконання коду. Live Server запускає сервер і вікно браузера за замовчуванням, в якому відображається результат виконання коду без необхідності самостійного оновлення вікна браузера.

Редактор VSCode також має портативну версію. Це буває в нагоді, коли редактор не встановлений на учбових комп'ютерах в аудиторіях і вчитель не має можливості самостійно встановити цю програму.

Для цілей вивчення вебдизайну також можна використовувати так звані «песочниці», тобто он-лайн редактори, на кшталт CodePen (codepen.io), JSFiddle (jsfiddle.net), JS Bin (jsbin.com) тощо.

У процесі навчання звісно ж активно використовується браузер, який зазвичай має засоби розробника (Firefox, Opera, Chrome та ін.). Ці засоби як правило активуються натисканням клавіши [F12]. Ми рекомендуємо засоби розробника від браузера Firefox. Також активно можна використовувати різноманітні розширення для браузера, наприклад, Web developer, What Font, Stylus та ін.

Будування вебсторінки робиться у відповідності до графічного макету, який в свою чергу був створений у графічному редакторі, зазвичай у Adobe Photoshop або, в останній час, у Figma. У дисципліні розглядається тематика визначення параметрів вебсторінки по графічному макету, а також «витягнення» ресурсів з макету для створення вебсторінки. Для того, щоб не прив'язуватися до графічної програми, якої може і не бути інстальовано на учбовому комп'ютері, можна поступити таким чином: заздалегідь створити необхідний графічний макет і зберегти його як зображення у файл, наприклад, у форматі JPG. Відкриваємо це зображення прямо у браузері. Для визначення параметрів макету можна скористатись розширеннями для браузера: Measure-it – для визначення розмірів, ColorZilla – для визначення кольорів.

Вивчення матеріалу курсу, зокрема, робиться відповідно до принципу систематичності й послідовності [3]. Матеріал подається від простого до складного. Навички набуваються, зокрема, завдяки повторенню виконання відносно великої кількості однотипних завдань. На наш погляд, для більш якісного засвоєння

матеріалу, наступні практичні завдання повинні містити елементи попередніх завдань.

Кожне практичне заняття забезпечується методичними матеріалами, які мають таку орієнтовну структуру: номер, тема, мета практичного заняття, учбові питання, завдання, хід роботи, довідкові матеріали, стислі теоретичні відомості, контрольні питання та/або тест. Також може бути включений розділ «Методичні рекомендації», в якому пояснюється як працювати, власно, з методикою виконання. Розділ «Стислі теоретичні відомості» може бути відсутніми, у зв'язку з суто практичним характером вивчення матеріалу. Розділ «Хід роботи» також може бути відсутнім, тому що сутність завдання буде полягати у самостійному визначенні порядку дій студентом.

У зв'язку з тим, що «друковані» методичні матеріали, тобто ті, які містять текст, зорієнтовані на електронну публікацію, вони забезпечені великою кількістю кольорових скріншотів. Також методика виконання містить велику кількість фрагментів відформатованого коду. Підкажемо, що при копіюванні фрагментів коду з редактора VSCode, форматування тексту зберігається.

Також необхідно в методичних матеріалах показати скріншот виконаного завдання, щоб студент міг контролювати правильність виконання своєї роботи.

Рекомендуємо створити завдання для студентів за варіантами для контролю доброчесності.

Крім надання методичного матеріалу у вигляді тексту, зображень, прикладів, не треба забувати про анімаційні зображення і відео. Наявність цих матеріалів підвищить наочність і зрозумілість матеріалу, який треба засвоїти.

Таким чином, з огляду на наш практичний досвід, вважаємо, що застосування прийомів і методів, які були розглянуті вище, дозволить підвищити результативність засвоєння матеріалу і набуття навичок студентами.

Список використаних джерел:

1. Пасічник О. Г. Основи вебдизайну / О. Г. Пасічник, О. В. Пасічник, І. В. Стеценко. Київ: Видавнича група BHV, 2009. 336 с.
2. Освітня програма «Кібербезпека». Одеса. 2021. URL: https://drive.google.com/file/d/1y3Lr0ZQvKFG3Okwevc-daNSLAKXLN2Ry/view
3. Джеджула О. М. Методика викладання у вищій школі: навчальний посібник / Вінниця: ВНАУ, 2020. 208 с.

ЕЛЕКТРОННЕ ГОЛОСУВАННЯ

Трач Я. М.

студентка 1 курсу факультету міжнародно-правових відносин
Національного університету «Одеська юридична академія»

Під електронним голосуванням розуміється можливість використання електронних обчислювальних засобів під час виборів та підрахунку голосів. Власне кажучи, сам розвиток обчислювальної техніки почався зі створення ще у XIX столітті спеціальних пристроїв (табуляторів), призначених для прискорення процесу підрахунку результатів перепису населення.

Наприклад, до електронного голосування можна віднести процедуру реєстрації числа тих, хто проголосував за того чи іншого кандидата за допомогою спеціальних комп'ютерів, завданням яких є реєстрація та підрахунок голосів.

Крім того, до електронного голосування можна віднести і онлайн-голосування (інтернет-голосування) – коли люди мають можливість проголосувати за допомогою різних комп'ютерних пристроїв дистанційно, не відвідуючи виборчу дільницю. Такий варіант голосування, до речі, набув великого поширення під час недавньої пандемії.

Електронне голосування може використовуватися як для локальних підрахунків голосів (наприклад, під час нарад в організаціях), так і для проведення виборів або референдумів у масштабах країни. І якщо перший варіант активно використовується, то другий все ще вважається експериментальним.

Хоча жодна країна все ще не вирішила використовувати для проведення виборів виключно онлайн-голосування, деякі країни, такі, як Естонія, Швейцарія та Канада, вже надали виборцям, на їх вибір, можливість голосувати через Інтернет. Крім того, у Монголії з 2015 року стало можливим голосування на референдумах за допомогою SMS [1].

Технологія електронного голосування призначена для прискорення підрахунку бюлетенів, скорочення кількості персоналу, необхідного для ручного підрахунку голосів та забезпечення більшої доступності участі у виборах для виборців (виборці можуть голосувати незалежно від свого фактичного розташування). Як наслідок, застосування електронного голосування дозволить підвищити загальну явку виборців за рахунок громадян, які проживають за кордоном або у сільській місцевості далеко від виборчих дільниць. Крім того, таке голосування дозволить брати участь у виборах й особам з інвалідністю з обмеженими можливостями пересування.

Результати електронного голосування стануть відомі одразу після закінчення процедури голосування.

Крім того, електронне голосування дозволяє значно знизити витрати на організацію та проведення виборів.

На жаль, електронне голосування пов'язане і з великою кількістю ризиків та можливих проблем, таких, як можливість фальсифікації результатів виборів та порушення таємниці голосування. Навіть тільки сама можливість таких порушень призведе до зниження довіри населення до виборчих процедур і результатів виборів, причому навіть до їх початку.

З цієї причини ще до введення в країні електронного голосування потрібне проведення цілої низки заходів, що дозволяють підвищити довіру населення до процедур проведення юридично значущих дій через мережу Інтернет.

23 серпня 2021 року набрав чинності Закон *України "Про внесення змін до Закону України* «Про *Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», що дозволив прирівняти цифрові паспорти у* застосунк*у «Дія» до паперових* [2].

Таким чином, Україна стала другою у світі країною (після Естонії) з електронними паспортами. До слова, Естонія є країною, чия система електронного уряду по праву вважається однією з кращих.

Минулого року майже половина виборців на парламентських виборах в Естонії проголосувала через Інтернет. До парламенту Естонії через Інтернет були подані рекордні 247 232 голоси, 43,8% загального числа.

А перші вибори з використанням системи інтернет-голосування пройшли в Естонії в 2005 році. Це були загальнонаціональні вибори місцевих органів влади, тоді 9317 виборців проголосували через Інтернет.

Технологія має на увазі використання естонської ID- карти. Це смарт-карта зі вбудованим електронним чіпом, підтримуваним державною інфраструктурою відкритого ключа, що надає право як безпечної видаленої аутентифікації, так і юридично обов'язковому цифровому підпису.

Але широку популярність цей спосіб отримав в 2011 році з додаванням можливості голосування через мобільний телефон (використовувалася спеціальна SIM- карта і захист PIN- кодом).

Естонська система інтернет-голосування на виборах Естонії виділяється і низкою інших особливостей. Вона дозволяє виборцям голосувати в період дострокового голосування (від шести до чотирьох днів до дня виборів) і міняти свій електронний голос необмежене число разів.

Говорячи про безпеку, уряд Естонії, звичайно ж, приділив цьому аспекту належну увагу, але, тут важливо розуміти, що Естонія - маленька країна (на останніх виборах проголосувало всього 561 131 людина) і на відміну від США і країн західної Європи, включаючи Україну, вона не представляє особливого інтересу для вороже налагоджених держав [3].

Іншими словами, потенційна загроза втручання іноземних держав в естонські вибори украй низька. З урахуванням цього не варто особливо розраховувати, що в майбутньому такий спосіб голосування стане широко поширеним по всьому світі.

Враховуючи недавню історію з втручанням Росії в американські президентські вибори, знадобиться ще немало часу, щоб вирішити усі труднощі і створити систему, несприйнятливу до усіх відомих на сьогодні.

Президент Володимир Зеленський пообіцяв в майбутньому надати українцям можливість голосувати на виборах за допомогою смартфону через Інтернет. На жаль, ніяких термінів він не повідомив, відмітивши лише, що в майбутньому така можливість обов'язково з'явиться [4].

Отже, можна зробити такий висновок, що електронне голосування все ж таки має більше переваг, ніж недоліків. По - перше - це високий рівень зручності для виборця, швидкий підрахунок голосів, точний реєстр виборців, економія коштів та інше. Саме тому, на нашу думку, електронне голосування було б досить актуальним саме у нашій країні.

Список використаних джерел:

1. Benefits and risks of e-voting and on-line voting URL: https://cutt.ly/RHQ09WY
2. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. №5492-VI. *Відомості Верховної Ради України*. 2013. №51. Ст. 716.
3. Почти половина избирателей на недавних парламентских выборах в Эстонии проголосовала через интернет. URL: https://cutt.ly/YHQ2Hjv
4. Вторые после Эстонии. Украина введет электронные паспорта в марте, а в будущем украинцы смогут голосовать на выборах через интернет. URL: https://cutt.ly/iHQ2Ncz

Науковий керівник: доцент Чанишев Р.І.

СФЕРИ ЗАСТОСУВАННЯ ЧАТ-БОТІВ

Трофименко О. Г.

кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Можливими нішами для чат-ботів є сервіси інформування учасників певних груп і колективів, рутині інформаційні процеси виборчих кампаній та закладів вищої освіти, особливо на початку навчального року, служби бронювання і купівлі квитків, служби підтримки з доставки товарів, їжі, квітів тощо. Сфери і способи застосування ботів найрізноманітніші і залежать від креативності розробників. Чат-боти є незамінними помічниками у будь-якій сфері, де наявні великі обсяги комунікації з клієнтами. До того ж, при розробці чат-ботів можна інтегрувати платіжні системи для онлайн-оплати при прийомі замовлень, що дозволяє суттєво покращити, спростити та пришвидшити взаємодію з клієнтами, позбавляє від потреби телефонувати їм. Застосування чат-ботів суттєво економить

час, позаяк клієнт, який звернувся за підтримкою, отримує відповідь миттєво в режимі 24/7, без очікування на підключення оператора. При цьому він не стикається зі спамом, зайвими балачками, нав'язливими закликами, а отримує лише корисну інформацію.

Нині однією з основних сфер застосування чат-ботів є розсилка рекламних оголошень, акційних пропозицій тощо. Тобто чат-боти використовують як потужний інструмент маркетингу. Дослідження [1] свідчить, що 90% повідомлень у месенджерах відкривають протягом 90 секунд після отримання, а у п’ять разів перевищує показники ефективності e-mail та SMS. При цьому витрати на розсилку набагато нижчі. Тому компанії зацікавлені в розширенні бази контактів і збільшенні обсягів продажів засобами відповідних чат-ботів. Крім того, застосування чат-бота дозволяє суттєво знизити навантаження і витрати на службу підтримки, позаяк автоматизує обробку простих, часто повторюваних запитів від клієнтів. При цьому відбувається паралельне опрацювання необмеженої кількості заявок. Це дозволяє розвантажити команду і залучати менеджерів тільки за потреби вирішення складних завдань, тим самим оптимізувати витрати на персонал.

У сфері статистики боти корисні тим, що можуть автоматично відслідковувати ціни на акції, перегляди сторінок вебсайту компанії або кількість контактів, які було створено за попередній день, формувати статистичні дані у зручний користувачу формат тощо.

Одною з важливих можливостей чат-ботів є можливість збирати інформацію про користувачів, відслідковувати їхні дії, а потім за потреби проаналізувати їхні звички. Зібрані в процесі діалогу дані про користувачів дозволяють персоналізувати пропозиції і розсилку. Бот може використовуватися як інструмент налагодження смартпроцесів усередині компанії і при цьому взаємодія з ним відбувається у звичному і зручному інтерфейсі певного месенджера, наприклад, Telegram. Чат-бот засобами API дозволяє підключитись до зовнішніх систем і синхронізуватись із корпоративними системами, наприклад: CRM, ERP, «Google Таблиці» тощо.

У медицині чат-боти можуть використовуватись, насамперед, для швидкої дистанційної попередньої діагностики. Крім того, засоби штучного інтелекту можуть використовуватись для аналізу даних здоров'я як окремих пацієнтів, так і прогнозування тенденції поширення вірусних захворювань на період сезонних коливань та можливих епідемій. Майбутнє в області охорони здоров'я залежить від здатності впровадження таких технологій [2], адже збір даних при опитуванні пацієнтів відбувається віддалено, що знижує навантаження на лікарів та зменшує ймовірність поширення інфекційних захворювань. Крім того, успішно зарекомендували себе чат-боти в загальній та клінічній психології як додаткові засоби медичної допомоги [3]. Такі чат-бот для психічного здоров’я дозволяють користувачам говорити про все, що вони хочуть, і є достатньо розумними, щоб задавати змістовні питання та відповідати на них. Їх метою є психологічна

допомога людям, які борються з депресією, особливо якщо їм не вистачає уваги і нема з ким поговорити про свою проблему.

У навчальному процесі існують різні види чат-бітів. Одні з них здатні миттєво відповісти на численні питання абітурієнтів під час вступу до закладу вищої освіти (запитання про вступну кампанію, спеціальності та їх різницю, гуртожитки, історію факультету тощо). Інші мають за мету полегшити та пришвидшити студентам будь-якого курсу пошук інформації під час навчання (про розклад занять, навчально-методичні матеріали, розміщення аудиторій, навчальний процес тощо) та допоможуть швидко вирішити будь-які організаційні питання, адже швидке отримання відповідей на запитання – одна з найбільш бажаних функцій у процесі навчання студента. Дослідження свідчать про високу довіру студентів до цієї технології та задоволеність її використанням [4]. Успішним є використання чат-бота у галузі професійної орієнтації для пошуку майбутньої роботи, здатного обробляти будь-які запити природною мовою та підвищуючи мотивацію учнів до отримання певної професії у віртуальному інформаційному середовищі [5].

У галузі рекрутингу чат-бот вважається ефективною комунікаційною системою, яка успішно спрощує роботу менеджерів по персоналу та рекрутерів, автоматично збираючи та систематизуючи відповідні компетенції, навички та досвід під час автоматичного онлайн опитування кандидатів. Адже людські ресурси (HR) будь-якої організації відіграють важливу роль у будівництві та зростанні компанії, визначаючи ефективних та компетентних працівників [6]. Технологія, керована ШІ, перетворює складні проблеми на спрощені рішення. Такого роду чат-боти вдало визначають найкращих кандидатів, збільшують кількість заявок, адже працюють у режимі 24/7, автоматично планують проведення співбесід і відповідають на запитання кандидатів на роботу.

З винаходом чат-ботів, які є важливою сферою в галузі ШІ та обробки природних мов, організації стали ширше їх залучати для виконання робіт, орієнтованих на спілкування без будь-якого людського втручання [7]. Чат-боти налагоджують стосунки, відповідають на запитання і сприяють кращому порозумінню серед працівників організації з урахуванням відповідних проблем, впливають на процес прийняття рішень в організації.

Отже чат-боти можуть мати різне призначення і мати різний функціонал, і саме від нього залежить вибір платформи, в якій він буде працювати, і засобів розробки. Після визначення вимог до створюваного чат-бота, залежно предметної області, треба розробити комунікаційну архітектуру, яка дозволить вибудувати ієрархію контенту для спілкування. Для цього варто провести опитування серед групи людей цільової аудиторії, структурувати контент і змоделювати схему діалогу бота, зібрати інформацію, необхідну для можливого подальшого навчання бота з метою повноцінного ведення ним діалогу і розуміння ним різних варіантів одного й того самого поняття для формування коректних відповідей.

Список використаних джерел:

1. Vynogradova O. V., Drokina N. I., Darchuk V. G. Feasibility of messenger-marketing for promotion of goods and services on the internet. *Economics. Management. Business.* 2020. No 1(31). P. 11-20. DOI: 10.31673/2415-8089.2020.011120.
2. Bulla Ch., Parushetti Ch., Teli A., Aski S., Koppad S. A Review of AI Based Medical Assistant Chatbot. 2020. Vol. 2. P. 1-14. DOI: 10.5281/zenodo.3902215.
3. Hussna A., Laz A., Sikder M., Uddin J., Tinmaz H., Esfar-E-Alam A. PRERONA: Mental Health Bengali Chatbot for Digital Counselling. *Intelligent Human Computer Interaction.* 2021. P. 274-286. DOI: 10.1007/978-3-030-68449-5_28.
4. Pesonen J. 'Are You OK?' Students' Trust in a Chatbot Providing Support Opportunities. *International Conference on Human-Computer Interaction HCII 2021: Learning and Collaboration Technologies: Games and Virtual Environments for Learning.* 2021. P. 199-215. DOI: 10.1007/978-3-030-77943-6_13.
5. Tischenko A. Developing a chatbot as a virtual assistant to motivate students to get a profession. *Ergodesign.* 2021. P. 140-144. DOI: 10.30987/2658-4026-2021-2-140-144.
6. Majumder S., Mondal A. Are chatbots really useful for human resource management? *International Journal of Speech Technology.* 2021. DOI: 10.1007/s10772-021-09834-y.
7. Trofymenko O., Prokop Y., Loginova N., Zadereyko A. Taxonomy of Chatbots. *International Scientific and Practical Conference «Intellectual Systems and Information Technologies» (ISIT2021)*. September 13-19, 2021, Odesa, Ukraine. P. 181-185.

РОЛЬ МАТЕМАТИЧНИХ ДИСЦИПЛІН В ПІДГОТОВЦІ ФАХІВЦІВ ДЛЯ ІТ ГАЛУЗІ

Чепурна О. Є.

доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Для реалізації стратегічної мети України – побудови інноваційно-інвестиційної моделі розвитку, та відновлення країни – необхідно проаналізувати, які фактори цьому будуть сприяти. Загальновідомо, що найважливішими факторами, які забезпечують конкурентні переваги економіки, є наука, освіта, культура, технології. Саме освіта спрямована на формування, розвиток трудового потенціалу України та побудову ефективної моделі «економіки знань». Від освіти, особливо вищої, залежить майбутній розвиток науки, технологій, у тому числі інформаційних.

Вагомий внесок у дослідження освітнього фактору розвитку трудового потенціалу та економіки України зробили вітчизняні науковці С. Бандур, Д. Богиня, О. Грішнова, Б. Данилишин, Г. Дмитренко, М. Долішній, Е. Лібанова, Л. Лісогор, О. Макарова, С. Ніколаєнко, В. Новіков, В. Онікієнко, та інші [1].

Поділ освіти на фундаментальну, яку дає університет і професійну комерційну, яку дають спеціалізовані та авторизовані навчальні центри інформаційних технологій, вимагає від вищих навчальних закладів більш ретельно ставитися до

складання освітніх програм, наповнювати їх дисциплінами спрямованими як на формування професійних навичок, так і високоякісну математичну підготовку. Останнім часом нові технології стали наукомісткішими – точніше, математикоємними. У багатьох сферах людської діяльності стало активніше застосовуватися математичне моделювання різних процесів. Фізична реалізація експериментів, експериментальна перевірка висунутих гіпотез є дуже дорогими, як правило, потребують значних людських та матеріальних ресурсів. Імітація експериментів на математичних моделях, виявлення закономірностей під час багаторазового моделювання виявляється на порядки дешевшим. На основі математичних моделей розробляється відповідне програмне забезпечення, що реалізує математичну модель об'єкта та математичні методи, що дозволяють знайти оптимальне рішення. І якщо ми замінюємо фізичний експеримент математичним, то маємо бути впевнені, що їхні результати збігаються. У такій ситуації фахівцю з ІТ-технологій обійтися без глибоких математичних знань та обчислювальних методів майже не можливо.

На наш погляд, математична та алгоритмічна підготовка потрібна майбутнім фахівцям у галузях, пов'язаних з машинним навчанням, нейронними мережами, штучним інтелектом. Найбільш корисні отримати знання з наступних розділів: математичний аналіз, лінійна алгебра, теорія ймовірності, лінійне програмування та методи лінійної та нелінійної оптимізації, теорії ігор, теорія алгоритмів, технології і методи високопродуктивних обчислень.

Як правило, студенти с певним скепсисом ставляться до необхідності вивчати математичні дисципліни, більш уваги приділяють саме програмуванню. Але знання мов програмування, вміння написання кодів ще не гарантує високу конкурентоспроможність на ІТ ринку. Ні для кого не є секретом, що математика розвиває критичне мислення, удосконалює навички аналізу та синтезу, ґрунтовне розуміння математичних принципів та законів, практичне застосування математичних методів, сприяє розвитку програміста, як фахівця, який не тільки якісно виконує завдання, але стає в змозі самостійно ставити задачу, та створювати власний продукт, що підвищує його конкурентоздатність на ринку и робити свій вклад в економіку рідної країни.

Список використаних джерел:

1. Заюков І. В. Підготовка фахівців з інформаційних технологій – основа розвитку економіки знань України. URL: http://conf.vntu.edu.ua/humed/2010/txt/Zayukov.php/

РАНДОМІЗАЦІЯ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ВИХОДІ ПРОГРАМНОГО ГЕНЕРАТОРА

Щербина Ю. В.

доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Постановка проблеми

Результатом розвитку сучасної комп'ютерної техніки є те, що, на відміну від минулого сторіччя, моделювання складних стохастичних систем перетворилось із другорядного етапу проектування на один із основних способів розроблення процесів сучасного виробництва, управління інфраструктурними об'єктами та економічною діяльністю.

Для створення комп'ютерної моделі процесу, який протікає в умовах відсутності абсолютної визначеності, в першу чергу необхідно мати у своєму розпорядженні генератор з абсолютно рівномірним розподіленням випадкових чисел на його виході. Числові послідовності з іншими типами розподілення ймовірностей формуються саме із рівномірного розподілення за принципом, описаним у [1]. Зважаючи на те, що обчислювальні пристрої – це детерміновані автомати, вони здатні формувати на виході лише псевдовипадкові числа (ПВЧ) з обмеженим періодом повторення *T*. Щоб така послідовність виглядала як випадкова, період має бути достатньо великим, тобто він повинен на порядки перевищувати довжину процесу, що підлягає моделюванню. На даний момент ця проблема розробниками програмного забезпечення вже вирішена. Так, наприклад, генератор ПВЧ, побудований з використанням чисел Мерсена (MT), має період повторення 2^{19937} – 1 біт. Що ж стосується рівномірності розподілення чисел на його виході, то проведені експерименти показують, що такий генератор не тільки не може бути використаний для криптографічних перетворень, але й не відповідає вимогам моделювання. Те ж саме сказати і про лінійний конгруентний генератор (LCG) [2].

Ціль дослідження. Зважаючи на те, що двоетапна система моделювання дуже чутлива до рівномірності розподілення чисел на виході обраного генератора, і те, що генератори LCG і MT, включені у більшість середовищ програмування, не відповідають вимогам рівномірності за критерієм Пірсона χ^2 [3], єдиним виходом вбачається пошук такого способу постоброблення потоку псевдовипадкових чисел на виході генератора, який відповідав би відповідність вимогам моделювання.

Визначення способу постоброблення потоку псевдовипадкових чисел

В середині минулого сторіччя фон Нейманом було зроблене обґрунтоване зауваження про неприйнятність фізичних генераторів випадкових чисел для задач моделювання через технічні труднощі можливості повторної реалізації отриманої вибірки. З урахуванням цього положення, були запропоновані такі

алгоритми, як метод середніх квадратів [4] та лінійний конгруентний метод. У той же період Д. Кнутом [2], було показано, що вони теж не забезпечували необхідної рівномірності сформованого потоку. Оскільки зробити ідеальний генератор практично не можливо, ідея постоброблення як для генераторів реальних випадкових чисел, так і для генераторів ПВЧ залишається актуальною і донині.

Для потреб постоброблення використовують спеціальні прості коректори (Ad hoc simple correctors), алгоритми видалення (Extractor algorithms) та хеш-функції (Whitening with hash functions). Загальною вимогою до всіх способів постоброблення є мінімізація обчислювальних ресурсів, для їх реалізації.

Прикладом простого коректора може бути коректор, описаний фон Нейманом, де він пропонує об'єднувати пару бітів, отриманих від незалежних джерел за принципом: якщо біти співпадають (00 або 11), то вони скасовуються, комбінації бітів 01 відповідає 0-й вихідний біт, а комбінації 10 відповідає 1-й вихідний біт. Максимальна ефективність такого алгоритму складає в середньому 4 вхідних бити на 1 вихідний біт. Саме у цій роботі фон Нейманом було зроблено акцент на труднощах генерації випадкових десяткових чисел.

Видалення (або відбілювання) передбачає зменшення кореляції символів на виході джерела ентропії. Воно збільшує однорідність та рівномірність розподілення символів у складі потоку на виході генератора. Для його реалізації використовують такі хеш-алгоритми як MD5, SHA-1, SHA-2, SHA-256 або SHA-512.

Екстракторами випадковості називають алгоритми, які перетворюють низькоякісний потік вхідних величин у майже рівномірний потік числових символів за допомогою невеликої кількості гарантовано випадкових бітів. Спосіб такого перетворення описано в роботі Люка Тревісена [5]. Він вводить поняття мінімальної ентропії, яка характеризує нерівномірність розподілення величини X у діапазоні $\{0,1\}^n$, де n – це бінарна комбінація на виході джерела. У разі рівномірного розподілення всі комбінації будуть рівно імовірними і ентропія буде максимальною.

Ще один спосіб підсилення випадковості величин вихідного потоку генератора ПВЧ запропоновано в роботі [6]. Він основується на постфільтрації через деякий детермінований процес. Ідея полягає в тому, щоб за рахунок використання еластичних функцій розділити вихідні символи на випадкові і "недостатньо випадкові". По суті, пропонується "просіяти" вихідний потік, щоб видалити із нього «зайві» числа, які «потворять» загальну картину рівномірності розподілення ймовірностей. Такий спосіб достатньо просто реалізувати, оскільки він вимагає невелику кількість обчислювальних ресурсів.

Використання критерію Пірсона χ^2, передбачає розділення діапазону чисел на виході генератора на k – інтервалів з подальшим обчисленням показника рівномірності по правилу $\chi^2 = (n_i - Np_i)^2/Np_i$. Тут N – це розмір вибірки, p_i – ймовірність попадання в i-тий інтервал, яка у разі рівномірного розподілення

дорівнює $1/k$, n_i – реальна кількість чисел, що попала в i-тий інтервал, а Np_i – очікувана кількість чисел, що має попасти в i-тий інтервал.

Математичне очікування величини, що має попасти в сегмент, обмежений умовами $x_{min} \le n_i < x_{min}$ визначається як $m_i = (x_{min} + x_{min})/2$. Тоді кількість чисел, що попали в i-тий сегмент s_i, орієнтовно буде дорівнювати величині $s_i^* = n_i^* m_i$. Тут x_{min} і x_{min} відповідні межі кожного з інтервалів. Звичайно, що кожного разу ця сума буде або менше, або більше s_i^* але суттєвої різниці не буде. Це дає можливість сформулювати наступний алгоритм. Якщо сума чисел s_i^*, що попали в i-тий сегмент гістограми перевищує величину s_i^*, то всі інші числа які в нього попадають пропускаються. Звичайно, що кількість чисел в сегментах залишиться різною, але нерівномірність вибірки стане меншою.

На рисунку 1 наведені результати випробувань вибірки довжиною N = 1024 дійсних десяткових псевдовипадкових чисел на виході MT генератора до і після постоброблення описаним способом. В останньому разі для 5% точності показник χ^2 = 03438, що менше критичного значення χ^2 = 7.2609.

Висновки

Найчастіше для сучасного комп'ютерного моделювання використовуються програмні пакети Boost, Glib, C++, Python, Ruby, R, PHP, MATLAB та їм подібні. Всі вони написані на мові C++ і використовують її генератори ПВЧ. Зважаючи на це, хорошим варіантом є будування моделей стохастичних процесів саме на цій мові, використовуючи програмні середовища Visual Studio або QT5, до складу яких входить велика кількість додаткових бібліотек, що містять різноманітні генератори ПВЧ.

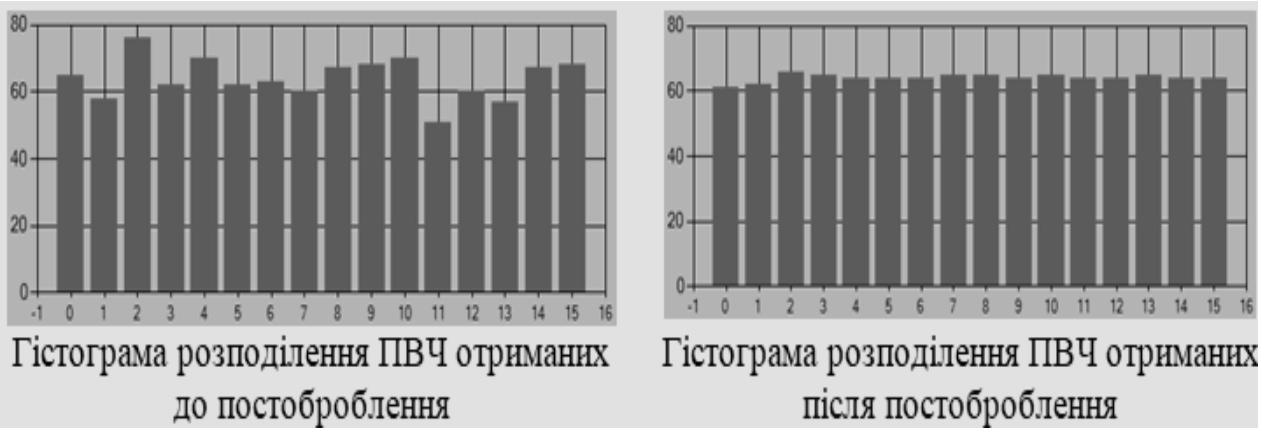


Рис. 1. Гістограма розподілення ПВЧ отриманих за допомогою функції uniform_real_distribution <> mersenne(0, 1)

Щоб забезпечити задану якість моделювання, необхідно попередньо виконати перевірку якості потоку на виході обраного генератора на предмет рівномірності розподілення сформованих чисел і, якщо є необхідність, провести додаткову його рандомізацію.

Список використаних джерел:

1. Mark A. Pinsky, Samuel Karlin. An Introduction to Stochastic Modeling, Fourth Edition., Academic Press, 2010. URL: https://faculty.ksu.edu.sa/sites/default/files/an_introd_to_stoch_modeling_4th_ed.pdf.
2. D. E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998. URL: https://doc.lagout.org/science/0_Computer%20Science/2_Algorithms/The%20Art%20of%20Computer%20Programming%20%28vol.%202_%20Seminumerical%20Algorithms%29%20%283rd%20ed.%29%20%5BKnuth%201997-11-14%5D.pdf.
3. J. H. Ahrens, U. Dieter, A. Grube, Pseudo-random numbers. Computing 6 (1970) 121-138). URL: https://doi.org/10.1007/BF02241740.
4. J. von Neumann. Various techniques for use in connection with random digits. Applied Math Series, Notes by G. E. Forsythe, in National Bureau of Standards, Vol. 12, 36 – 38, 1951. URL: https://mcnp.lanl.gov/pdf_files/nbs_vonneumann.pdf.
5. Trevisan L. Extractors and Pseudorandom Generators 1999. Journal of the ACM URL: http://theory.stanford.edu/~trevisan/pubs/extractor-full.pdf.

ПРОГРАМНІ ЗАСОБИ РОЗРОБКИ ЧАТ-БОТІВ

Ярош Є. В.

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

На сьогодні люди все частіше звертаються до чат-ботів. Нині за умов війни люди масово почали використовувати чат-боти для інформаційної боротьби з ворогом, отримання корисної інформації про роботу волонтерів чи про прихистки для людей у різних регіонах. Чат-боти допомагають підбирати музику та книжки, купувати різноманітні товари та квитки онлайн. Крім того, вони використовуються для імітації спілкування з живою людиною, як персональні асистенти, юридичні консультанти та навіть психотерапевти. Експерти прогнозують чат-ботам грандіозний розвиток в найближчі роки та порівнюють цей бум з розвитком вебу та соціальних мереж свого часу [1, 2]. Саме тому розробка чат-ботів є доволі актуальною.

Чат-боти можуть мати різне призначення і різний функціонал, і саме від цього залежить вибір платформи, в якій вони працюватимуть, і вибір засобів розробки. За призначенням розрізняють чат-боти для розмов на широкий спектр тем та чат-боти, орієнтовані на діалог тільки за певною тематикою. За функціоналом чат-боти розділяють на 3 види: інформаційно-комунікаційні, «питання – відповідь» та функціональні [3].

Інформаційно-комунікаційні чат-боти призначені виключно для інформування людей, щоб поділитися інформацією про спеціальні пропозиції та знижки,

допомогти підібрати товар або послугу тощо. Поширено для розробки таких чат-ботів використовують мову програмування Java. Особливістю програм на Java є те, що вони можуть запускатись на будь-яких комп'ютеризованих пристроях, які працюють під різними операційними системами, причому без повторної компіляції коду. Для їх реалізації необхідно встановити середовище для виконання Java Runtime Environment. Для управління залежностями можна скористатись фреймворком Apache Maven і підключити залежності Telegram Bots і Lombok в pom.xml [4]. Для того щоб чат-бот формував і відправляв відповіді, варто скористатись методом update.getCallbackQuery(), який через CallbackQuery дозволяє передавати дані [5].

Чат-боти «питання – відповідь» призначені формувати та надавати прості відповіді за принципом «одне питання – одна відповідь») [3]. Зручно розробку таких ботів реалізовувати багатоцільовою кросплатформною мовою програмування Python у середовищі розробки PyCharm [6], яке має аналізатор коду, графічний налагоджувач, інтегрований тестер модулів, інтеграцію із системами контролю версій, а також підтримує використання Django для веброзробки та Anaconda для аналізу даних [7]. Початком першого етапу реалізації є створення такого бота в системі месенджера Телеграм та отримання API токену. Наступним кроком є підключення бібліотек telebot, chatterbot та chatterbot_corpus до програмного середовища PyCharm. Бібліотека chatterbot_corpus дозволяє легко і швидко тренувати бот для подальшого спілкування [8]. Python-бібліотека chatterbot містить засоби генерування автоматизованих відповідей на введенні користувачем тексти запитів. При цьому для отримання різноманітних типів відповідей chatterbot використовує різні алгоритми навчання машин, що значно полегшує розробку інтелектуальних чат-ботів та «автоматизує» вільне спілкування з користувачами, наприклад, у вигляді переписки.

Функціональні чат-боти надають користувачам можливість швидко, без залучення сторонніх засобів виконати якісь функціональні дії, наприклад, переказати гроші на рахунок, уточнити статус замовлення за його номером тощо [3]. Такі чат-боти широко використовують у браузерних та комп'ютерних іграх та не лише в них. Для розробки функціональних чат-ботів варто використовувати мови програмування JavaScript або C#. Можливості мови JavaScript сильно залежать від середовища, в якому вона працює. Найкраще використовувати JavaScript для інтерактивних чат-ботів у браузерних іграх в поєднанні з платформою Node.js та її бібліотекою node-telegram-bot-api [9, 10]. Що стосується розробки чат-ботів засобами мови C#, середовища Visual Studio та фірмової платформи розробки чат-ботів від Microsoft Bot Framework, то вони мають зручні і потужні засоби розробки чат-ботів. Інтеграція шаблону Bot Framework у Visual Studio та встановлення відповідного пакету SDK дозволить розробляти розмовні чат-боти на базі штучного інтелекту (AI) [11]. Крім того, платформи Azure Bot Service та Azure Table Storage від Microsoft містять не лише засоби програмної розробки чат-ботів, а й керування станом у середовищі Azure Cloud для

публічного доступу через різні канали інтеграції (Messenger, MS Teams, Slack та ін.) для інтерактивного спілкування в усіх різновидах чат-ботів.

Отже, чат-боти можуть бути розроблені різними програмними засобами, які дозволяють створити web API. Програмування при розроблені чат-бота переважно стосується бекенду, який забезпечує отримання повідомлень або запитів користувача, формування та повернення їм коректних відповідей та пропозицій. Великий вибір сучасних різноманітних фреймворків та сервісів можуть суттєво допомогти у створенні якісного чат-бота.

Список використаних джерел:

1. Чатботи - хто вони? URL: http://surl.li/bwqyw.
2. 11 корисних чат-ботів у Telegram у період війни. URL: https://vogue.ua/article/culture/lifestyle/11-korisnih-chat-botiv-u-telegram-u-period-viyni.html.
3. Трофименко О.Г., Прокоп Ю.В., Задерейко О.В., Логінова Н.І. Класифікація чат-ботів. Системні технології. 2022. № 2 (139). С. 147-159. DOI: 10.34185/1562-9945-2-139-2022-14. URL: https://journals.nmetau.edu.ua/index.php/st/issue/view/120/87.
4. Создание Telegram-бота на Java: от идеи до деплоя. URL: https://javarush.ru/groups/posts/504-sozdanie-telegram-bota-na-java-ot-idei-do-deploja.
5. Telegram-бот на Java для самых маленьких — от старта до бесплатного размещения на heroku. URL: https://habr.com/ru/post/528694/
6. Футбольный телеграм бот на Python (1/4): Подготовка и настройка бота. URL: https://pythonru.com/primery/telegram-bot-na-python-ustanovka-i-nastrojka
7. MyCookBot от ProTelegram. URL: https://protelegram.ru/2016/08/25/mycookbot/
8. Создание чат-бота на Python. URL: https://pythonist.ru/sozdanie-chat-bota-v-python/
9. Які відмінності між node.js та node? URL: https://uk.waldorf-am-see.org/891726-what-are-the-differences-between-BHQKYU
10. Как написать Телеграм-бота на JavaScript. URL: https://htmlacademy.ru/blog/articles/telegram-bot
11. Microsoft Chat Bot – Tips And Tricks. URL: https://www.c-sharpcorner.com/article/microsoft-chat-bot-tips-and-tricks/.

Науковий керівник: доцент Трофименко О. Г.

Секція 2. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ: СОЦІАЛЬНИЙ, ПРАВОВИЙ І ТЕХНІЧНИЙ АСПЕКТ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ СТЕГАНОАНАЛІТИЧНИХ АЛГОРИТМІВ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ

Ахмаметьєва Г.В.

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Розвиток інформаційних технологій та впровадження цифрового документообігу в усі сфери людської діяльності сприяє накопиченню значної кількості конфіденційної інформації на серверах компаній, підприємств, організацій, що потребує її додаткового захисту. За останні роки був зроблений великий крок вперед в області стеганографії, яка досліджує засоби прихованого захисту інформації шляхом вбудови цифрових водяних знаків, організацію каналів прихованого зв'язку. Саме прихована передача повідомлень за допомогою стеганографічних методів становить найбільшу небезпеку, оскільки виток конфіденційних даних може призвести до катастрофічних наслідків – зловмисник може отримати доступ до персональних даних працівників і клієнтів установ та використати їх для скоєння злочинів. Особливу небезпеку становить використання стеганографічних методів в умовах воєнного стану, коли чутлива критична інформація може опинитися в руках ворога шляхом її прихованої передачі через відкриті месенджери або інтернет-ресурси у вигляді невинного зображення або відео. Для запобігання витоку інформації через приховані канали зв'язку слід застосовувати стеганоаналітичні алгоритми, спрямовані на виявлення факту наявності вбудованого повідомлення в будь-які цифрові контейнери.

Одним з найбільш використовуваних контейнерів в стеганографії є цифрове зображення завдяки наявності в ньому надмірної інформації та можливості приховування значного обсягу даних. Однак з метою ускладнення виявлення наявності додаткової інформації в контейнері стеганоаналітичними алгоритмами, часто вкладення повідомлення відбувається з малою пропускною спроможністю прихованого каналу зв'язку (ППС). Це значно зменшує обсяг даних, що слід передати, однак забезпечує більш надійний захист повідомлення, оскільки його наявність в контейнері складніше виявити.

Однією з ефективних розробок для виявлення вкладення в цифрових зображеннях є стеганоаналітичний метод Color Triads, опис якого наведений в [1], що показав високу ефективність для визначення вбудованих повідомлень методом LSB при малих значеннях ППС (менше 0,5 біт/піксель). В даній роботі проведений експеримент виявлення факту наявності повідомлень, вбудованих стеганографічними алгоритмами WOW [2], S-UNIWARD [3], MiPOD [4], за допомогою алгоритмічної реалізації методу Color Triads, та порівняння результатів з

сучасними аналогами. Вибір алгоритмів WOW, S-UNIWARD та MiPOD обумовлений їх доступністю в мережі та широким використанням в наукових публікаціях при тестуванні стеганоаналітичних алгоритмів.

При проведенні обчислювального експерименту вбудовування повідомлення в цифрові зображення здійснюється в одну довільно обрану складову кольору з ППС 0.4, 0.2 і 0.1 біт/піксель алгоритмами S-UNIWARD, MiPOD і WOW. За результатами стеганоаналізу сформованих стеганоповідомлень були отримані помилки першого роду (False Negative FN), наведені в таблиці 1, які вказують на пропуск стеганоповідомлень. Помилки другого роду (False Positive FP) – визначення незаповненого контейнера як стеганоповідомлення, склали 0,49%.

Таблиця 1. Помилки першого роду (FN) виявлення наявності/відсутності повідомлення в цифровому зображенні алгоритмічною реалізацією методу Color Triads, %

Стеганографічний алгоритм	ППС, біт/піксель			
	0,4	0,2	0,1	0,05
S-UNIWARD	0,16	0,66	4,11	14,45
MiPOD	0,33	1,32	8,70	14,12
WOW	0	0,82	3,78	11,33

З таблиці 1 видно, що стеганоаналітичний алгоритм Color Triads забезпечує високу ефективність виявлення вбудованих повідомлень при значеннях ППС 0,1 біт/піксель та вище методами S-UNIWARD, WOW та MiPOD.

Порівняння ефективності виявлення наявності повідомлень будемо визначати за точності детектування наявності/відсутності повідомлень в зображенні серед всіх зображень, які включають як стеганоповідомлення, так і незаповнені контейнери. Результати порівняння ефективності для стеганоаналітичного алгоритму Color Triads і сучасних аналогів наведені в таблиці 2.

Таблиця 2. Порівняння точності детектування цифрових зображень стеганоаналітичним алгоритмом Color Triads та сучасними аналогами, %

	ППС, біт / піксель	SRM + EC [5]	CNN [5]	CNN + SRM + EC [5]	SCA-TLU-CNN [6]	FLD [7]	LSMR [8]	LASSO [9]	Color Triads
S-UNIWARD	0.4	77,95	90,95	84,13	87,19	–	–	–	99,67
	0.2	–	–	–	77,76	66,58	66,58	63,29	99,43
	0.1	59,00	76,64	61,12	67,80	–	–	–	97,70
	0.05	–	–	–	60,00	–	–	–	92,53
MiPOD	0.4	76,11	90,74	84,35	–	–	–	–	99,59
	0.2	–	–	–	–	66,79	66,93	63,31	99,09
	0.1	57,87	78,12	59,76	–	–	–	–	95,41
	0.05	–	–	–	–	–	–	–	92,69
WOW	0.4	–	–	–	90,41	–	–	–	99,51
	0.2	–	–	–	83,09	67,11	67,33	63,06	99,35
	0.1	–	–	–	75,58	–	–	–	97,87
	0.05	–	–	–	65,5	–	–	–	94,09

З таблиці 2 видно, що алгоритм Color Triads набагато перевищує результати аналогів: точність виявлення наявності/відсутності вбудованого повідомлення перевищує 92% навіть для ППС 0,05 біт/піксель.

В роботі наведений порівняльний аналіз розробленого раніше автором стеганоаналітичного алгоритму з сучасними аналогами. Показано, що алгоритм Color Triads є ефективнішими за сучасних аналогів, особливо при значеннях ППС 0,1 біт/піксель та вище.

Список використаних джерел:

1. Akhmametieva, A.: Steganalysis of digital contents, based on the analysis of unique color triplets. Annales Mathematicae et Informaticae, no. 47, 3-18 (2017).
2. Holub, V., Fridrich, J.: Designing Steganographic Distortion Using Directional Filters. In: 2012 IEEE International Workshop on Information Forensics and Security (WIFS 2012), pp. 1-6. IEEE, Tenerife, Canary Islands (2012).
3. Holub, V., Fridrich, J., Denemark, T.: Universal Distortion Function for Steganography in an Arbitrary Domain. EURASIP Journal on Information Security (Section: SI: Revised Se-lected Papers of ACM IH and MMS 2013), 1-13 (2014).
4. Sedighi, V., Cogranne, R., Fridrich, J.: Content-Adaptive Steganography by Minimizing Statistical Detectability. IEEE Transactions on Information Forensics and Security, vol.11, iss.2, 221-234 (2016).
5. Couchot, J.-F., Couturier, R., Salomon, M.: Improving Blind Steganalysis in Spatial Domain Using a Criterion to Choose the Appropriate Steganalyzer Between CNN and SRM+EC. In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 327-340. Springer, Rome, Italy (2017).
6. Jian Ye, Jiangqun Ni, Yang Yi: Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Transactions on Information Forensics and Security, vol.12, iss.11, 2545-2557 (2017).
7. Kodovsky, J., Fridrich, J., Holub, V.: Ensemble classifiers for steganalysis of digital media. Information Forensics and Security, IEEE Transactions, vol.7, no.2, 432-444 (2012).
8. Fong, D.C.-L., Saunders, M.: LSMR: An iterative algorithm for sparse least-squares prob-lems. SIAM Journal on Scientific Computing, vol. 33, no. 5, 2950-2971 (2011).
9. Cogranne, R., Sedighi, V., Fridrich, J., Pevný, T.: Is Ensemble Classifier Needed for Steganalysis in High-Dimensional Feature Spaces? IEEE International Workshop on Information Forensics and Security (WIFS 2015), pp.1-6. IEEE, Rome, Italy (2015).

СКЛАДНОЩІ ТА ПРОБЛЕМИ У РОЗВИТКУ СУЧАСНОЇ КРИПТОГРАФІЇ

Бойко В.Д.

кандидат технічних наук, доцент, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Пастернак Ю.Ю.

заступник декана факультету кібербезпеки та інформаційних технологій,
асистент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Останні дослідження в області криптографії є важливою інвестицією в майбутнє. Особливо на тлі досягнень сучасного криптоаналізу і постійного зростання обчислювальних потужностей, однак це зростання потужностей має й іншу сторону, більші потужності дозволяють зловмисникам швидше робити атаки грубою силою та вирішувати складніші задачі. Також, незважаючи на те, що криптографія являє собою вже доволі стару науку, вона досі має багато невирішених проблем, кількість яких через технологічний прогрес лише зростає. Через це необхідно постійно розробляти нові криптографічні алгоритми та удосконалювати вже існуючі.

Криптографія та криптоаналіз наразі є найважливішими аспектами розвитку інформаційної безпеки у сучасному світі, а сучасна криптографія зводиться до математичних обчислень, тому, незважаючи на нещодавнє формування сучасної криптографії, вона вже має низку невирішених проблем. Разом із стрімким розвитком технологій та обчислюваних можливостей, збільшуються й можливості зловмисників. Багато алгоритмів, які вважалися алгоритмами з високою крипостійкістю, зараз розкриваються за допомогою атаки брутфорсом. Також враховуючи появу хмарних сервісів та віртуалізації, з'являються зовсім нові вимоги до інформаційної безпеки.

Традиційні алгоритми криптографії були побудовані шляхом поєднання великої кількості простих перетворень, що забезпечує стійкі характеристики кінцевого алгоритму. З тих пір як практичні основи були закладені Горстом Фойстелем, принципи одноключових алгоритмів майже не змінилися. Зміни мали переважно кількісний характер та базувалися на появі більш потужних комп'ютерів. В сучасній криптографії все зовсім по-іншому: надійність алгоритмів базується на недоведеній обчислюваній неможливості ефективного вирішення математичних задач. Наприклад, стійкість RSA криптосистеми базується на складності проблеми факторизації великих чисел, а надійність сучасних схем електронного підпису будується на складності проблеми логарифмування в обмежених полях [3].

Враховуючи це, можна виділити основні сучасні проблеми шифрування:

Обмежена кількість робочих схем. На відміну від класичних алгоритмів криптографії, які можна створювати в необмеженій кількості, комбінуючи різні

елементарні перетворення, сучасні схеми базуються на визначенні «нерозв'язної» проблеми. Як наслідок, ми маємо лише невелику кількість діючих схем з відкритим ключем.

Постійне збільшення розмірів блоків даних та ключів за рахунок розвитку математики та інформатики. Під час розробки RSA криптосистеми, 512-розрядні числа вважалися достатніми, а зараз це не менше 4 Кбіт.

Потенційно ризикова основа. Наразі доведено зв'язок між більшістю обчислюваних проблем, тому у разі якщо одна з сучасних криптосистем буде зламана, то і інші також будуть зламані.

Відсутність далекої перспективи. Передбачуваним кінцем сучасної криптографії є винахід квантового комп'ютеру, хоча поки вони існують лише в теорії.

Сучасні дослідження в сфері криптографії, безумовно, шукають способи вирішення цих проблем. Але криптографічні алгоритми – це лише побудова для створення систем та протоколів. Майже усі відомі вразливості у відомих криптосистемах були пов'язані саме з недоліками проектування та реалізації, тому разом з пошуком та розробкою нових алгоритмів важливу роль також відіграє й якість роботи розробників та проектувальників криптосистем.

Сьогоднішня криптографія повністю побудована на математиці, а головна мета, яку переслідує математика в криптографії це криптографічна стійкість, тобто можливість витримувати теоретичні та практичні атаки на шифр. Таким чином, системи шифрування, які використовуються в криптографічних системах в всесвітній мережі (RSA, ElGamar, Shamir та ін.) використовують останні досягнення теорії чисел та алгебри. Зламати їх – вирішити найскладніші математичні задачі.

Деякі проблеми існуючих криптографічних методів може вирішити, так звана, квантова криптографія. Це відносно новий напрямок досліджень, який дозволяє використовувати ефекти квантової фізики для створення секретних каналів передачі даних. У квантовій криптографії використовується фундаментальна особливість квантових систем, яка полягає в принциповій неможливості точного з'ясування стану такої системи. На сьогоднішній день вже декілька корпорацій пропонують перші комерційні системи квантової криптографії, але самі квантові системи ще не скоро увійдуть у масове використання. Незважаючи на це, квантові системи вже зараз можуть знайти застосування задля захисту особливо важливих каналів зв'язку [4].

Список використаних джерел:

1. Miller V**.** Uses of elliptic curves in cryptography. Advances in Cryptology – CRYPTO'85, Lecture Notes in Computer Science, 218 (1986), pp. 417–426.
2. Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 48 (1987), pp. 203–209.
3. Kahn D. The Codebreakers – The Story of Secret Writing. – Simon and Schuster,1996. – 1200p
4. Fred Cohen A Short History of Cryptography – 1987.

ВИКОРИСТАННЯ КЛІТИННИХ АВТОМАТІВ В ШИФРУВАННІ ДАНИХ

Бойко В.Д.

кандидат технічних наук, доцент, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Пастернак Ю.Ю.

заступник декана факультету кібербезпеки та інформаційних технологій,
асистент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Клітинні автомати - самостійні об’єкти теоретичного вивчення, і вони ж - інструмент для моделювання в науці і техніці. В основі популярності клітинних автоматів лежить їх порівняльна простота в поєднанні з великими можливостями для моделювання сукупності взаємопов'язаних однорідних об'єктів. Крім того, клітинні автомати, будучи паралельними структурами, підходять для моделювання дискретних паралельних процесів, для створення паралельних алгоритмів обробки інформації і становлять інтерес в якості основи обчислювальної техніки з високопаралельною архітектурою.

У криптографії клітинним автоматам можна знайти багато застосувань, починаючи з генерації псевдовипадкових послідовностей та закінчуючи створенням алгоритмів шифрування, повністю побудованих на клітинних автоматах та їх властивостях. З кожним днем клітинні автомати привертають дедалі більшу увагу криптографічної спільноти в зв'язку з розпаралеленістю їх структури, яка дозволяє збільшувати швидкість роботи і пропускну здатність апаратних реалізацій криптоалгоритмів. Цікаві перспективи з'являються також при використанні клітинних автоматів для побудови криптографічних алгоритмів, не вимогливих до обчислювальних ресурсів.

Всі спроби використовувати клітинні автомати в конструкції блокових шифрів безпосередньо в якості циклової функції шифрування упиралися насамперед в питання зворотності клітинного автомату. Якщо автомат є зворотним, зворотне перетворення може бути реалізовано також за допомогою клітинного автомату.

Найбільш суттєві результати, пов'язані з питаннями зворотності, отримані для класичних клітинних автоматів, заданих на нескінченних решітках. Було доведено, що для одномірних клітинних автоматів завдання алгоритмічного розпізнавання зворотності є вирішуваним. Був побудований алгоритм розпізнавання, що має експонентну складність. Пізніше були побудовані алгоритми для розпізнавання оборотності одномірних клітинних автоматів, що мають поліноміальну складність. Однак для клітинних автоматів на решітках з двома і більше вимірами таких алгоритмів немає. Було встановлено, що в загальному випадку ця задача є алгоритмічно нерозв'язною в тому сенсі, що не існує алгоритму, який для будь-

якого автомата завжди закінчував би свою роботу в кінцевий час і давав би правильну відповідь. Також досліджувалися межі між класами клітинних автоматів, для яких властивість оборотності є алгоритмічно розв'язаною, і тими, для яких вона є алгоритмічно нерозв'язною. Отримано критерій можливості розв'язання властивості оборотності для класів клітинних автоматів фіксованою розмірності і з фіксованим числом станів осередку. Було отримано критерій можливості розв'язання властивості оборотності в класі клітинних автоматів з фіксованим шаблоном сусідства.

Побудова зворотних клітинних автоматів в розмірностях більших, ніж 1, досить важка. Відомо декілька типів оборотних двомірних клітинних автоматів, основними з яких є блокові клітинні автомати і клітинні автомати 2-го порядку. Автомати цих типів відрізняються від класичних клітинних автоматів, проте доведено, що вони можуть бути емульовані класичними клітинними автоматами навіть із більшим розміром околиці та числом станів осередку [2].

В криптографічних цілях, як правило, застосовуються клітинні автомати з решітками кінцевого розміру. Питання зворотності для таких клітинних автоматів завжди можна розв'язати, і основне завдання полягає в знаходженні прийнятних критеріїв для перевірки зворотності, алгоритмів для реалізації зворотного перетворення і оцінки складності цих алгоритмів. Наразі ці питання дуже мало досліджені, результатів дуже небагато, а ті, які є, не стимулюють швидке просування і швидких успіхів у цьому напрямку. Також проводилися спроби дослідити властивість оборотності двовимірних клітинних автоматів на безлічі конфігурацій.

Головну роль у побудові надійного алгоритму блокового шифрування на основі клітинного автомату відіграє вибір самого автомату. Узагальнений клітинний автомат має два параметри, які потрібно обрати розробнику: структуру графу та локальну функцію зв’язку.

Вибір структури графу впливає на криптостійкість алгоритму. Граф не повинен мати паралельних та антипаралельних дуг та усі його вершини повинні мати одну й ту саму півступінь заходу та півступінь виходу, тобто графу потрібно бути сильно регулярним. Вибраній локальній функції потрібно ускладнювати криптоаналіз алгоритму. Вона повинна значно залежати від усіх своїх аргументів, бути рівноважною та мати максимально велику нелінійність.

Також слід зазначити, що клітинні автомати за самою своєю природою дуже підходять для використання в конструкціях хеш-функцій, кодів виявлення модифікації інформації та кодів перевірки справжності повідомлення. В цьому напрямку запропоновано досить багато конструкцій. Так, деякі праці на цей рахунок пропонують різні конструкції хеш-функцій, що базуються на використанні клітинних автоматів [7].

Що стосується криптосистем з відкритим ключем на базі клітинних автоматів, то їх відомо дуже небагато. Завдання зворотності багатовимірних клітинних автоматів лежить в основі стійкості деяких криптосистем з відкритим ключем.

Наразі існує ще багато способів використання клітинних автоматів, які не були вивчені та можуть мати велике значення у майбутніх криптографічних дослідженнях.

Список використаних джерел:

1. Toffoli T. Computation and construction universality of reversible cellular automata // Journal of Computer and System Sciences. 1977. 15, №2. pp. 213–231.
2. Wolfram S. Cellular Automata as Models of Complexity // Nature. 1984. 311. pp. 419–424.
3. Wolfram S. Universality and complexity in cellular automata // Physica D. 1984. 10. pp. 1–35.
4. Wolfram S. Computation theory of cellular automata // Commun. Math. Phys. 1984. 96. pp. 15–57.
5. Wolfram S. Cryptography with Cellular Automata // Advances in Cryptology: Crypto ‘85 Proceedings. Lecture Notes in Computer Science, vol. 218. Springer-Verlag, 1986. pp. 429–432.
6. Wolfram S. Theory and applications of cellular automata: Including selected papers 1983-1986. River Edge, NJ.: World Scientific Publishing Co., Inc., 1986.
7. Wolfram S. Cellular Automata and Complexity. – Addison-Wesley, Reading, 1994.
8. Wolfram S. A new kind of science. – Champaign, Ilinois: Wolfram Media Inc., 2002. 1280 p.

ПРОБЛЕМА КВАЗІ-ОДНОКОРИСТУВАЛЬНОГО РЕЖИМУ ПРИ ЕКСПЛУАТАЦІЇ ОПЕРАЦІЙНИХ СИСТЕМ СІМЕЙСТВА MICROSOFT WINDOWS

Бойко В.Д.

кандидат технічних наук, доцент, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

У доповідях [1] та [2] розглядалася можливість та практичні аспекти переходу академічної освіти на використання open source програмного забезпечення. Було обґрунтовано актуальність та необхідність переходу на відкрите програмне забезпечення[1]. Були розглянуті причини, через які навчальні процеси у вищих закладах виявилися насичені піратським (зламаним, або не ліцензованим явно) програмним забезпеченням, необхідність і невідворотність далі строго контролю за ліцензійною чистотою використовуваного програмного забезпечення. У [2] докладно розбиралися практичні аспекти переходу на відкрите програмне забезпечення: описаний перехід (відкрите ПЗ, відкриті формати даних) був організований поступово та послідовно. Як базова система використовувався, заснований на Debian GNU/Linux, дистрибутив операційної системи Ubuntu.

Перехід на нове програмне забезпечення дозволив вирішити ще одну проблему, а саме - питання роботи в квазі-однокористувальному режимі, поширеному в операційних системах сімейства Windows.

Управління користувачами та правами під Windows є досить заплутаною і незручною процедурою, тому серед користувачів поширений квазі-однокористувацький режим, коли більша частина роботи відбувається під одним налаштованим користувачем, при цьому найчастіше задля зручності цього користувача створюють (або виділяють йому права) адміністратора системи [3], [4].

Цей режим роботи є широко поширеним серед користувачів операційних систем сімейства Microsoft Windows, тому не дивно, що робота в такому режимі також набула поширення в комп'ютерних класах більшості навчальних закладів [5].

При цьому операційна система на робочих місцях комп'ютерного класу використовується в режимі "одна роль операційної системи для всіх працюючих за комп'ютером користувачів". Часто комп'ютерний персонал намагається поліпшити ситуацію встановлюючи різне обмежує функціональність стороне ПЗ, що саме собою представляє проблему.

Експлуатація операційної системи у згаданому вище режимі "один користувач (одна роль) операційної системи для всіх працюючих за комп'ютером користувачів" призводить до того, що комп'ютер у лабораторії може використовуватися як робоче місце відразу декількома студентами (найчастіше – різних курсів), при цьому, оскільки механізми поділу користувачів не використовуються, їх файли, системні налаштування та установки неминуче змішуються. Це призводить одразу до кількох негативних явищ.

Перше можна назвати "каузальним плагіатом" - вільний доступ до чужих робочих файлів провокує на їх часткове або повне використання у своїй роботі, яке може бути як імпульсною реакцією, так і заздалегідь спланованою поведінкою.

Такій поведінці найчастіше намагаються протистояти шляхом відмови від постійного зберігання файлів на робочому місці та переходу на використання сторонніх носіїв (найчастіше usb флеш-драйвів, або хмарних сервісів). При цьому робочий процес виглядає так: файли копіюються на робоче місце, з ними відбувається робота, далі вони зберігаються назад на флеш-драйв (або в хмару), після чого файли, що залишилися на робочому місці, видаляються.

Це вирішує проблему лише частково (використання файлів так чи інакше залишає слід, при запланованому заздалегідь плагіаті на комп'ютер може бути встановлено malware ПЗ з функціоналом запису дій користувача), при цьому в свою чергу створює додаткові проблеми. Наприклад, флеш-драйви дуже швидко перетворюються на переносники та розповсюджувачі шкідливого ПЗ. Крім того, копіювання файлів займає час і забирає енергію, "від'їдаючи" її у навчального процесу та працюючи таким чином як своєрідне "тертя" або "комп'ютерна бюрократія". Найчастіше використання таких заходів швидко сходить нанівець і

комп'ютер перетворюється на хаотичне нагромадження різних файлів, яке у системних адміністраторів отримало окремий термін - "файлопомийка".

Виникнення "файлопомийки" призводить до негативних явищ другої категорії, яке, за нашими спостереженнями, добре пояснюється "теорією розбитих вікон" (англ. broken windows theory) [6]. Відповідно до положень цієї теорії, дрібні порушення правил у суспільно-доступній системі (розбите вікно в будівлі), провокує все більше таких порушень (що характеризуються ємною фразою "іншим можна, а мені не можна?") в результаті система позбавляється більшої частини свого ресурсу (в будівлі не залишається жодного цілого вікна) [7]. Ця теорія спочатку використовувалася пояснення механізмів і динаміки криміногенної обстановки у межах і у цій ролі часто критикувалося, проте, її становища цілком можна поширити використання операційної системи без поділу на користувальницькі ролі.

Рідко виходить так, що всі користувачі, що працюють на робочому місці комп'ютерного класу, суворо дотримуються писаних і неписаних правил використання файлового простору, налаштування програмного забезпечення та конфігурацію операційної системи. Порушення правил одним користувачем, провокує порушення правил іншими користувачами. Такі порушення накопичуються, що призводить до того, що поведінка користувачів одного комп'ютера стає все менш щадною та поважною по відношенню один до одного. Іноді таке ставлення може спричинити ворожість між користувачами. При цьому дрібні порушення можуть переростати у цілеспрямований вандалізм. Це відбувається рідко, хоча автору кілька разів доводилося спостерігати розвиток конфліктів, які починалися з встановлення заставок на робочих столах провокуючого змісту і закінчувалися використанням шкідливого програмного забезпечення та викраденням особистих даних з кешу браузера (або просто з незакритої по забудьку сесії роботи).

Очевидні недоліки безпеки та незручності такого режиму використання операційної системи користувачі та адміністратори системи прагнуть компенсувати за рахунок встановлення додаткового ПЗ, що виконує функції як забезпечення безпеки, так і заборони доступу до налаштувань і ресурсів операційної системи. Однак таке "блокуюче ПЗ" не тільки має сумнівну ліцензійну чистоту і потенційно несе в собі додаткові загрози безпеці, але насамперед сильно ускладнює навчальний процес, оскільки для встановлення та оновлення необхідного програмного забезпечення (а також відкриття прав та доступу, яке це ПЗ вимагає) доводиться звертатися до системного адміністратора. Це негативно позначається як на самому навчальному процесі, так і на навичках, які студенти отримують, які часто втрачають ініціативу і самостійність. Замість дослідження операційної системи, її режимів роботи та налаштувань, студент опиняється у "дитячому манежі", будь-який вихід за межі якого вимагає звернення до сторонніх осіб.

Незважаючи на те, що "блокуюче ПЗ" створює помилкову ілюзію відносної безпеки операційної системи та навчального ПЗ, його механізми захисту та блокування розраховані на некваліфікованого користувача і досить просто обходяться, а крім того, створюють мінімальну перешкоду (або не створюють її зовсім) різного шкідливого ПЗ. Таке ПЗ не може завадити поширенню вірусів, троянів, хробаків тощо.

Можливості навести лад у такому сформованому процесі обмежені. У випадках вандалізму рідко вдається визначити конкретного порушника без складного та витратного за часом та ресурсами дослідження системних журналів. Наведення порядку у файлах та даних робочого місця також ускладнюється - кожен користувач вважає свої файли та налаштування цінними та активно пручається їх упорядкуванню.

За всієї зовнішньої незначності, такий режим експлуатації операційної системи та робочий процес у комп'ютерних класах загалом створює атмосферу безладу та хаосу та - згідно з "теорією розбитих вікон", знижує і якість навчального процесу та ентузіазм учнів, що є серйозною проблемою при підготовці кваліфікованих ІТ -Фахівців.

Список использованных источников:

1. Бойко В.Д. Вопросы перехода на свободное программное обеспечение в современном академическом образовании. In Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України), volume 1, pages 607--610, 2021.
2. В.Д. Бойко. Практические аспекты перехода на свободное программное обеспечение в современном академическом образовании. In О. В. Дикий, editor, Кібербезпека в сучасному світі : матеріали III Всеукр. наук.-практич. конф. (м. Одеса, 19 листоп., 2021 р.), page 148. Одеса : Видавничий дім «Гельветика», October 2021.
3. Add a work or school account as a separate windows user. URL: https://answers.microsoft.com/en-us/windows/forum/all/i-want-to-add-a-work-or-school-account-as-a/ee7caa6c-3b9a-43f0-b4eb-0f59f3fe26f7
4. The 21 worst tech habits - and how to break them – ARN. URL: https://www.arnnet.com.au/article/459900/21_worst_tech_habits_-_how_break_them/?fp=2&fpid=2
5. How (and Why) to Create a Separate Windows Account Just for School | PCMag URL: https://www.pcmag.com/how-to/how-and-why-to-create-a-separate-windows-account-just-for-school
6. Kelling G. L. et al. Broken windows //Atlantic monthly. 1982. Т. 249. №. 3. С. 29-38.
7. Harcourt B. E., Ludwig J. Broken windows: New evidence from New York City and a five-city social experiment //U. Chi. L. Rev. 2006. Т. 73. С. 271.

СОЦІАЛЬНА ІНЖЕНЕРІЯ В КОНТЕКСТІ РОЗУМІННЯ МЕТОДОЛОГІЇ ЩОДО АНАЛІЗУ ОЦІНКИ РИЗИКІВ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Василенко М. Д.

доктор фізико-математичних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Слатвінська В. М.

аспірантка кафедри господарського права та процесу Національного університету «Одеська юридична академія»

Інформаційне суспільство охоплює всі області людського та національного життя. Однак людство, яке стало широко використовувати телекомунікації і глобальні комп'ютерні мережі, не може передбачити можливості використання цих технологій. Соціальну інженерію можна представляти як метод керування діями індивіда без використання технічних засобів, що ґрунтується на використанні слабкостей людського фактору [1]. Соціальна інженерія побудована на використанні некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації, доводячи, що найслабкішою ланкою системи «безпеки – людина» залишається людина. З іншого боку, соціальну інженерію часто розглядають як незаконний метод отримання інформації, тому сьогодні її активно використовують в Інтернеті для отримання закритої інформації або інформації, що має достатню цінність. Тоді методи несанкціонованого доступу до інформації можна умовно поділити на категорії, коли використовують методи соціальної інженерії та ті, що, в певній мірі, існують без них. Тому створення політики безпеки захисту інформації від несанкціонованого доступу стало необхідною складовою загальної справи безпеки підприємства в контексті використання аналізу та управління ризиками. Аналіз ризику відноситься до процедури виявлення факторів ризику та оцінки їх значущості. Таким чином, ризик - це ймовірність настання певних небажаних подій, які негативно вплинуть на досягнення цілей конкретного бізнес-процесу. Аналіз ризику включає оцінку ризику і методи зниження ризику або пов'язаних з ним несприятливих наслідків. Існує два види аналізу ризику - якісний і кількісний, які доповнюють один одного. Якісний аналіз спрямований на визначення (ідентифікацію) факторів, секторів і видів ризику. Кількісний аналіз ризику повинен дозволяти визначити величину окремих ризиків і загальну величину ризику в цілому. Кінцевий результат якісного аналізу ризику, в свою чергу, забезпечує вихідну інформацію для кількісного аналізу. Однак кількісна оцінка ризику також є найбільш складною, оскільки потребує відповідної вихідної інформації та чіткої шкали оцінки ризику. Тематика застосування різних методів аналізу ризику в інформаційній безпеці розглядається в рамках курсу «Аналіз і управління ризиками», який читається на

факультеті кібербезпеки та інформаційних технологій НУ «Одеська юридична академія». Суть управління ризиками полягає в аналізі факторів ризику та прийнятті відповідних рішень щодо усунення ризиків. Фактори ризику використовуються при оцінці ризику і пов'язані з основними параметрами, зазначеними в міжнародних стандартах. Залежно від методології оцінки ризику, що використовується організацією, визначається метод аналізу та оцінки поданих параметрів. Загальний процес аналізу ризику складається з трьох етапів: підготовка до аналізу ризику, аналіз можливих сценаріїв аварії, визначення ступеня ризику і вибір рекомендацій з управління ризиком. Існує експертний метод оцінки ризику, який являє собою сукупність логічних і математико-статистичних методів і процедур обробки висновків групи експертів, при цьому висновки є єдиним джерелом інформації. І тут виникає можливість використання інтуїції, життєвого та професійного досвіду учасників опитування. Методи використовуються тоді, коли недолік або повна відсутність інформації не дає змоги використовувати інші можливості. Найбільш відомим серед цих методів став метод Делфі. Перевага цього підходу в тому, що якісний підхід дозволяє конкретно оцінити кожну ситуацію. У деяких випадках може бути важливіше ретельно розглянути різні фактори, що визначають ситуацію, ніж проводити систематичну кількісну оцінку. Такий підхід заохочує незалежне мислення членів комісії і дозволяє збалансовано оцінити питання.

До недоліків можна зарахувати надмірну суб'єктивність оцінок. При прийнятті рішень будь-які риси або переваги експертів можуть істотно впливати на підсумкові оцінки. Все ж таки основним обмеженням у використанні методу Делфі стає складність у підборі великої групи експертів, які мають необхідну компетенцію у досліджуваному питанні. Існують також статистичні методи оцінки ризику (наприклад, метрика ризику з використанням VaR), які визначають ймовірність втрат на основі статистичних даних за попередній період і встановлюють області (зони) ризику, фактори ризику та інші параметри ризику. Основна перевага статистичних методів полягає в тому, що можна аналізувати і оцінювати різні сценарії і розглядати різні фактори ризику в рамках одного підходу з урахуванням накопичених статистичних даних. Основні переваги методології метрики ризику полягають у тому, що ризик може бути виміряний універсально в різних умовах навколишнього середовища, оскільки ризик може бути виміряний в термінах ймовірності втрат, і що ризики окремих компонентів можуть бути об'єднані в одне значення для всього досліджуваного об'єкта з урахуванням різних факторів, що впливають на об'єкт. Позитивним аспектом є те, що втрати і пов'язані з ними ризики можна аналітично порівняти. Інформаційні методи оцінки ризиків, основним завданням яких можна виділити визначення ризиків, найбільш актуальних для конкретної інформаційної системи.

Розгляньмо новітні і найбільш поширені методи, включаючи CRAMM, RiskWatch і CORAS.

CRAMM (Метод аналізу та управління ризиками ССТА) був розроблений компанією Insight Consulting у відповідь на запит Центрального агентства з

комп'ютерів і комунікацій у Великобританії. Через деякий час була впроваджена версія CRAMM для громадянського суспільства, фінансових і комерційних організацій.

Аналіз ризику в CRAMM полягає у виявленні та визначенні рівня ризику на основі оцінки активів, загроз і вразливості активів; CRAMM забезпечує аналіз і документування вимог, пов'язаних з безпекою, обґрунтування витрат, пов'язаних зі створенням інформаційних систем, надмірні заходи захисту, що всі можливі ризики були визначені, що вразливості ресурсів були визначені і оцінений їх рівень, що загрози були визначені і оцінений їх рівень, і що заходи захисту засновані на формальному підході для забезпечення їх ефективності.

CRAMM ділить процедуру аналізу ризиків на три етапи: ідентифікація та оцінка активів. Оцінка ризиків (включаючи оцінку загроз і вразливості). Вибір і рекомендація захисних заходів. CRAMM має велику бібліотеку захисних заходів.

Переваги CRAMM включають комплексний підхід до оцінки ризиків, застосування методів оцінки загроз та вразливостей щодо довіреності, систему моделювання інформаційної системи, зручну для застосування в галузі інформаційної безпеки, багату базу знань про захисні заходи, універсальність та адаптованість до різних організаційних профілів, а також проведення аудиту відповідно до

Недоліком методу CRAMM є те, що для його використання потрібна спеціальна підготовка і висока кваліфікація аудиторів; CRAMM краще підходить для аудиту вже працюючих інформаційних систем, ніж систем, що знаходяться в стадії розробки; аудити CRAMM досить трудомісткі і можуть вимагати від аудиторів безперервної роботи протягом декількох місяців. Програмний інструментарій CRAMM створює велику кількість паперової документації, яка не завжди корисна на практиці; CRAMM не дозволяє користувачам створювати власні шаблони звітів або змінювати існуючі; база знань CRAMM не може бути доповнена користувачами не може бути доповнена користувачем, що створює деякі проблеми при адаптації її до потреб конкретної організації [1].

Метод RiskWatch був розроблений компанією RiskWatch Inc. у США за участю NIST, Міністерства оборони США і Міністерства національної оборони Канади. Вона підтримує програмні продукти для різних видів аудиту, включаючи відповідність ряду стандартів і керівних документів, класифікованих по областях застосування, таких як охорона здоров'я, банківський і фінансовий сектор і корпоративна безпека (за винятком стандарту PCI DSS, актуальність якого сумнівна за межами США).

Усі продукти RiskWatch використовують як базову платформу загальну для цього типу продуктів архітектуру. У спрощеному вигляді ця архітектура може бути виражена наступним чином: Велика база знань, що містить інформацію про активи, загрози, вразливості, види шкоди, засоби захисту та анкети для оцінки факторів ризику. Програмний інтерфейс для маніпулювання базою знань та оцінки ризиків на основі даних бази знань і результатів анкетування. Інтерфейсний

додаток для створення і заповнення анкет користувачів і генерації звітів за результатами оцінки ризиків.

У методі RiskWatch як показники для оцінки та управління ризиками використовуються прогнозовані середньорічні втрати (Annualized Loss of Expectancy, ALE) та оцінка повернення від інвестицій (Return on Investment, ROI).

Отже, можна зробити висновок, що можуть застосовувати комбінований підхід як найкращий підхід до оцінки ризиків інформаційної безпеки. Цей підхід включає в себе використання набору методів аналізу ризиків, що складається з методів, які найкраще підходять для конкретних областей конкретної організації. Наприклад, метод Дельфі добре підходить для CRAMM, оскільки він дозволяє враховувати специфіку конкретного об'єкта. Це дозволяє підвищити точність оцінки ризиків інформаційної безпеки за рахунок обліку всіх характеристик інформаційної системи. Тому розглянуті загальні методи аналізу ризиків можуть бути успішно застосовані до інформаційної безпеки, якщо їх адаптувати і вдосконалити.

Список використаних джерел:

1. Соціальна інженерія // Вікі-знання/Тернопіл. нац. техн. ун-т ім. Івана Пулюя. URL: http://wiki.tstu.edu.ua/Соціальна_інженерія.

СПОСОБИ ВИЯВЛЕННЯ SQL-ІН'ЄКЦІЙ

Васильєв Б. Г.

студент 1-го курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Перші відомості про SQL-ін'єкцію з'явилися у відкритому доступі в статті «Вразливості вебтехнологій NT», опублікованій ще в 1998 році. З 2000 року дану техніку почали широко застосовувати кіберзлочинці для взлому інтернет-сайтів. Сьогодні є багато технік експлуатації SQL-ін'єкцій для різних СКБД та застосунків на їх основі. За минулі кілька років, атаки, які були спрямовані на різні Web застосунки вимагали особливої уваги з боку захисного персоналу [1]. Все це відбувається через те, що наскільки б сильним не був між мережний захист або наскільки старанно б не латали "дірки" в існуючих програмах, все одно може статися, що розробники ПЗ не досить добре захистили свої програми, і зловмисники можуть використовувати це для злому порту. Існує два найбільш частовикористовуваних методів для нападів: SQL ін'єкція і міжсайтовий скріптніг.

SQL ін'єкція належить до методики вставки мета-симолів і SQL команд в поля введення на Web сторінках, у результаті чого відбуваються зміни виконання кінцевих SQL запитів [2, 27]. Такі напади в основному спрямовані на Web-сервера. Принцип дії міжсайтового скриптингу полягає у використанні

знаходження шкідливих програм в URL , через натискання користувачем на URL посилання.

У наших прикладах ми будемо використовувати програму IDS Snort і складемо регулярні вирази, відповідно правил щодо знаходження подібних різновидів атак. Написана величезна кількість правил для знаходження таких атак. Якщо треба знайти будь-який варіант SQL атаки, то треба уникнути спроби вводу будь-якого з мета-символів SQL типу одинарної лапки ('), крапки з комою (;) або подвійного тире (–). Точно такий же параноїдальний спосіб знаходження CSS атак складається з виявлення кутових дужок (<>), що вказують на HTML-тег. Але при подібних умовах є ймовірність того, що більшість вірних виразів, стануть виявлені як вірогідність атак. Щоб уникнути цього, слід дотримуватись більш конкретних умов перевірки і при цьому не приводити до неправильної ідентифікації. Кожна з таких умов може застосовуватися як безпосередньо, так і за допомогою команди Snort сигнатур, використовуючи ключове слово pcre. Відповідні сигнатури можуть також взаємодіяти з утилітами типу grep для перевірки файлів реєстрації на Web серверах. Але такий спосіб може застосовуватися, лише якщо застосунки використовують GET запити, тому що дані про POST запитах не зберігаються в файлах реєстрації.

Значним при виборі регулярного виразу для знаходження SQL ін'єкцій є те, що може застосувати зловмисник в полі введення або поле cookie. Ми повинні аналізувати всі вхідні дані користувача як підозрілі. Як було згадано раніше, найпростіше регулярний вираз, що застосовується для знаходження SQL ін'єкцій, змушений знаходити певні мета-символи SQL типу одинарної лапки або подвійного тире. Для знаходження таких символів і їх шістнадцяткових еквівалентів може застосовуватися наступні вирази:

Регулярний вираз для визначення SQL мета-символів:

/ (\% 27) | (\ ') | (\ - \ -) (\% 23) | (#) / ix </ TD <tr>

Пояснення: для початку виявляється шістнадцятковий еквівалент одинарної лапки або безпосередньо сама лапка, а також наявність подвійного тире. Відповідні мето-символи MS SQL Сервер і Oracle, що вказують на початок коментаря (тобто все що слід за цими символами - ігнорується). Додатково, в разі застосування MySQL, треба перевірити наявність '*' або його шістнадцятирічного еквіваленту. Звернути увагу на те, що при цьому не треба перевіряти шістнадцятковий еквівалент подвійного тире, тому що він не є мета-символом HTML і не буде закодований браузером. Також, якщо зловмисник буде намагатися вручну внести зміни замість подвійного тире на його шістнадцятковий еквівалент (використовуючи проксі типу Achilles), то в нападі з використанням SQL ін'єкції відбудеться збій. Зазначений вище вираз необхідно наступним чином додати до нового правила Snort:

alert tcp $ EXTERNAL_NET any -> $ HTTP_SERVERS $ HTTP_PORTS
(msg: "SQL Injection - Paranoid";

flow: to_server, established; uricontent: ". pl";

pcre: "/ (\% 27) | (\ ') | (\ - \ -) | (% 23) | (#) / i";

classtype: Web-application-attack; sid: 9099; rev: 5;) </ TD <tr>

У нашому випадку, ключове слово uricontent має значення".pl", тому що в середовищі, в якій проводяться наші випробування, CGI сценарії написані на Perl. Залежно від певного застосування це значення може бути ".php", або ".asp", або ".jsp", та ін. За допомогою описаного вище вираження ми виявляємо присутність подвійного тире, тому що бувають ситуації, коли SQL ін'єкція можлива навіть без застосування одинарної лапки. Прикладом може служити SQL запит з пропозицією where, що містить тільки числові значення:

select value1, value2, num_value3 from database

where num_value3 = some_user_supplied_number

В цьому випадку зловмисник може здійснити додатковий SQL запит, виконавши введення наступного вираження:

3; insert values into some_other_table

І нарешті, pcre модифікатори 'i' і 'x' використовуються, відповідно, для ігнорування регістра символів і пробілів (або знаків табуляції).

Описана вище сигнатура може бути доповнена для виявлення знака "крапка з комою". Однак крапка з комою може цілком нормально бути частиною HTTP трафіку. Для зменшення ймовірності неправильної ідентифікації, така сигнатура може бути модифікована, щоб спершу виявляти символ "=". Введення даних користувачем зазвичай відбувається як POST або GET запит, в якому вхідні поля будуть виглядати наступним чином:

username = some_user_supplied_value & password =

some_user_supplied_value

Тому при спробі SQL ін'єкції, даних користувача передував би знак = або його шістнадцятковий еквівалент.

Модифіковані регулярні вирази для виявлення SQL метасимволів

/ ((\% 3D) | (=)) [^ \ n] * ((\% 27) | (\ ') | (\ - \ -) | (\% 3B) | (;)) / i < / TD <tr>

Пояснення: відповідна сигнатура спочатку виявляє символ "=" або його шістнадцятковий еквівалент (% 3D). Після цього, ігноруючи роздільники рядків і прогалини, проводитиметься пошук входжень одинарної лапки, подвійного тире або крапки з комою. Зазвичай спроби SQL-ін'єкцій зводяться до використання одинарних лапок для управління початковим запитом. У більшості прикладів, наведених в статтях присвячених цього типу нападів, використовується рядок 1'or '1' = '1. Однак від виявлення цього рядка можна легко ухилитися, використовую значення типу 1'or2> --. Таким чином, єдиною постійною частиною таких виразів залишається символьне значення, що супроводжується одинарною лапкою, з подальшим за нею словом "or".

Регулярний вираз для типових SQL ін'єкцій

/ \ W * ((\% 27) | (\ ')) ((\% 6F) | o | (\% 4F)) ((\% 72) | r | (\% 52)) / ix </ TD <tr>

пояснення: \ W * - нуль або інші алфавітно-цифрові символи або символи підкреслення

(\% 27) | \ '- одинарна лапка або її шістнадцятковий еквівалент

(\% 6F) | o | (\% 4F)) ((\% 72) | r | (\% 52) - слово 'or' в різних комбінаціях верхнього і нижнього регістрів і їх шістнадцяткові еквіваленти.

Часто, застосування SQL-ін'єкцій при атаках на різні бази даних супроводжується використанням ключового слова "union". При використанні описаних раніше регулярних виразів ми можемо лише визначити наявність одинарних лапок або інших мета-символів SQL. Але далі ми будемо модифікувати наші регулярні вирази для визначення одинарної лапки і ключового слова "union". Те ж саме можна зробити і для інших ключових слів SQL типу 'select', 'insert', 'update', 'delete' та ін.

Регулярне вираження для визначення SQL ін'єкції з використанням ключового слова "union"

/ ((\% 27) | (\ ')) union / ix

(\% 27) | (\ ') - одинарна лапка і її шістнадцятковий еквівалент

union - ключове слово «union»

Подібні вирази можуть бути написані і для інших SQL запитів типу > select, insert, update, delete, drop та ін.

У разі якщо хакер виявив, що WEB додаток вразливе до SQL-ін'єкції, він почне експлуатувати цю уразливість. Якщо потрібна база даних зберігатися на MS SQL сервері, то хакер, швидше за все, спробує виконати одну їх багатьох небезпечних збережених або розширених збережених процедур. Назви таких процедур починаються, відповідно, з 'sp' або 'xp'. Як правило, він спробував би виконати розширену процедуру 'xp_cmdshell', що дозволяє виконувати через SQL сервер команди оболонки Windows. Права доступу до яких виконатися ця процедура будуть такі ж як і у облікового запису з якої запущений SQL сервер (зазвичай Local System). Додатково, зловмисник спробує внести зміни до реєстру за допомогою використання процедур xp_regread, xp_regwrite, і т.д.

Регулярний вираз для визначення SQL-ін'єкції на MS SQL сервері

/ Exec (\ s | \ +) + (s | x) p \ w + / ix </ TD <tr>

пояснення: exec - ключове слово необхідне для запуску збереженої або розширеної процедури

(\ S | \ +) + - один або кілька пробілів або їх еквіваленти закодовані HTTP

(S | x) p - символи 'sp' або 'xp' необхідні для ідентифікації збереженою або розширеної процедури, відповідно

\ W + - один або кілька алфавітно-цифрових символів або символів підкреслення, необхідних для завершення написання імені процедури.

Отже, деякі з таких виразів просто параноїдальні і видають попередження навіть при натяках на атаку. Але існує ймовірність, що використання таких сигнатур призведе до неправильної ідентифікації виразів. Для попередження цього,

необхідно змінити тривіальні сигнатури, забезпечивши їх додатковими перевірками і зробивши більш точними. Ми рекомендуємо використовувати ці регулярні вирази в якості відправної точки при налаштуванні будь-якої системи виявлення вторгнень.

Список використаних джерел:

1. Cyber Attacks 2020! : URL: https://sectigostore.com/blog/cyber-attacks-2020-notable-2020-cyber-attacks/
2. Корнага Я., Базака Ю., Мар'єнко Є. Способи оптимізації SQL–запитів для поліпшення роботи з базою даних в високонавантажених системах. *Адаптивні системи автоматичного управління.* Київ, 2020. Том 2 № 37. С.26-30.

Науковий керівник: доцент Лобода Ю.Г.

ЗАСОБИ ТА МЕХАНІЗМИ ПРОТИДІЇ DDOS-АТАКАМ

Величко С.В.

студентка 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

DDoS-атака або атака типу «відмова в обслуговуванні» (Distributed Denial of Service) спрямована на комп'ютерну систему з метою створення несприятливих умов для використання певних ресурсів або сервісів користувачами [1]. Класифікація атак відповідає базовій еталонній моделі взаємодії відкритих систем OSI [2]. На найнижчому мережевому (третьому) рівні для атаки відбуваються дії з використанням UDP-пакетів. Ідея атаки полягає у надсиланні безлічі UDP-пакетів (як правило, великого об'єму) на обрані або випадкові номери портів віддаленої комп'ютерної системи. При цьому для кожного отриманого пакета віддалена система повинна визначити відповідний додаток, переконатися у відсутності його активності та відправити відповідне повідомлення по протоколу ICMP «адресат недоступний». В результаті атакований хост виявиться перенавантаженим: у протоколі UDP механізм запобігання перенавантаженням відсутній, тому після початку атаки шкідливий трафік швидко захопить всю доступну смугу пропускання каналу хоста, перешкоджаючи при цьому трафіку від звичайного користувача.

На транспортному (четвертому) рівні атака полягає у відправці завеликої кількості SYN (*synchronize*) - запитів на встановлення підключень за протоколом TCP. При цьому зворотні пакети від обчислювальної системи з комбінацією флагів SYN+ACK (*acknowledges*) або ігноруються, або обробляються навмисно не вірно. Таким чином у системі створюється велика кількість напіввідкритих з'єднань збільшуючи при цьому чергу на підключення.

На рівні представлення даних (шостому рівні моделі взаємодії OSI) атака полягає у зловмисному використанні протоколу SSL. Для розшифрування даних

переданих по протоколу SSL необхідно витратити певну кількість ресурсів обчислювальній системі. Найчастіше механізм атаки полягає у хижацькому використанні механізму рукостискання SSL (коли на запит з'єднання надається новий запит і так далі), відправлення сміттєвих даних на сервер SSL або порушення певних функцій, пов'язаних із процесом узгодження ключа шифрування SSL.

На прикладному (сьомому) рівні атака відбувається через надсилання великої кількості HTTP(S) POST або GET запитів. На цьому ж рівні виконується атака на DNS-структуру шляхом надсилання порожніх запитів, або запитів на декілька DNS-серверів одночасно із зміненою адресою відправника на адресу об'єкта атаки.

Протидія DDoS атакам

Методи протидії DDoS-атакам можна розділити на пасивні та активні, а також на превентивні та реакційні. Перш за все необхідно відзначити профілактичні заходи щодо попередження DDoS-атак. Зрозуміло, що цей метод є управлінським, тим не менш аналіз можливих причин імовірних DDoS-атак є першим кроком до зменшення їх руйнівних наслідків. До управлінських методів варто віднести DDoS-атаку у відповідь.

Наступні методи полягають у використанні фільтрації за списками ACL (Access Control List) та використання мережевих екранів. Такі дії дозволяють загасити атаки або навіть їх припинити. Під час атаки деякий ефект можна отримати перенаправивши трафік на атакуючі комп'ютерні системи. Такий метод не буде мати ефекту якщо для атаки використовують заражені комп'ютерні системи (ботнет).

Для протидії DDoS-атакам на сьомому рівні моделі OSI компанія Cloudflare (https://www.cloudflare.com/) пропонує послуги з пом'якшення шкідливих дій. Служби Cloudflare працюють в якості посередника між відвідувачем вебсервісу та хостинг-провайдером Cloudflare, який, при цьому, виконує роль зворотного проксі. Для клієнтів компанія Cloudflare пропонує режим «Under Attack». Cloudflare стверджує, що це може пом'якшити розширені DDoS атаки 7-го рівня, представивши для цього обчислювальну задачу JavaScript, яку необхідно завершити браузером користувача, перш ніж користувач зможе отримати доступ до вебсайту. Окрім того, Cloudflare пропонує безкоштовну авторизовану систему доменних імен (DNS) для всіх клієнтів [3].

Не менш діючим є механізм оновлення системного та прикладного програмного забезпечення з можливістю повернення до попередньої версії. Варто розглянути в якості прикладного та системного програмного забезпечення вільне та відкрите програмне забезпечення [4], адже виявлення та виправлення недоліків серед цього класу програмного забезпечення проходить достатню кількість перевірок фахівцями різного рівня та спеціалізацій.

Сучасні захисні рішення забезпечують моніторинг трафіку, його фільтрацію, сприяють виявленню мережевих DDoS-атак різного типу. Вони блокують шкідливі пакети у трафіку, не перешкоджаючи доступу реальних користувачів, відстежують наявність аномалій, а у разі їх виявлення інформують хостера про можливу DDoS-атаку. Використання такого програмно-апаратного комплексу дозволяє підтримувати якість послуг, безперервність бізнес-процесів, а також знизити ризики для клієнтів.

Особливо ефективні є системи розподіленого захисту. Відповідне обладнання встановлюється у магістральних операторів, і якщо аналізатор атак фіксує напад на хост, або сервер, що захищається, він моментально транслює адреси атакуючих хостів іншим вузлам по всій мережі, і мережа починає працювати проти атакуючих хостів. Подібна система здатна відбити DDoS-атаки великої потужності.

Найбільш високопродуктивним і ефективним вважається застосування апаратних систем розподіленого захисту [5]. На приклад A10 Networks Thunder Threat Protection System володіє такими характеристиками як: автоматичний розрахунок фільтрів блокування та аналіз без попереднього налаштування або ручного втручання з подальшим блокуванням аномальної поведінки; 5-рівнева адаптивна ескалація політики, захист на основі машинного навчання; інтелектуальне виявлення сервісів з автоматичним призначенням політики пом'якшення наслідків; захист застосунків від DDoS-атак, що не вимагає спеціальної підготовки для застосунків і серверів; понад чотири десятки джерел інформації про загрози безпеки для миттєвого розпізнавання і блокування шкідливого трафіку.

Результатом використання сервісів захисту від DDoS-атак буде своєчасне виявлення та запобігання DDoS-атак, безперервність функціонування сайту та його постійна доступність для користувачів, мінімізація фінансових та репутаційних втрат від простоїв сайту чи порталу.

Список використаних джерел:

1. Захаров М. Як компаніям захиститися від DDoS-атак: пояснюють кіберексперти. З технічного боку. URL: https://cutt.ly/QHdBV0J
2. What is a DDoS Attack?. AWS. : URL: https://aws.amazon.com/shield/ddos-attack-protection/?nc1=h_ls.
3. Cloudflare DNS. *CLOUDFARE*. URL: https://www.cloudflare.com/dns/
4. Вільне та відкрите програмне забезпечення. URL: https://cutt.ly/uHdKnu4
5. A10 THUNDER TPS. URL: https://iitd.com.ua/tag/zashchita-ot-ddos-atak/

Науковий керівник: доцент Задерейко О.В.

БЕЗПЕЧНА КОММУНІКАЦІЯ В БЕЗДРОТОВИХ МЕРЕЖАХ WI-FI

Геращенко В.Д.

студент 1 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Wi-Fi (Wireless Fidelity) – технологія бездротової локальної мережі з основними діапазонами 2.4 ГГц (2412 МГц – 2472 МГц) та 5 ГГц (5160 – 5825 МГц) для взаємодії з мобільними пристроями [1].

Бездротові мережі мають достатньо велике поширення. У зв'язку з цим, кожен користувач має вміти організовувати безпечну комунікацію своєї мережі. Для забезпечення безпечного обміну даними у бездротових мережах було розроблено декілька основних технологій шифрування:

1. WEP – технологія шифрування, яка була розроблена у 1997 році Інститутом інженерів електротехніки та електроніки. Алгоритм забезпечував конфіденційність та захист персональних даних від неавторизованих користувачів із допомогою поточного шифру RC4, що мав високу швидкість шифрування [2].

2. WPA – технологія першого покоління, розроблена у 2003 році та була використана для заміни технології WEP, бо мала посилену безпеку даних та більш строгий контроль над користувачами. Технологія мала гарну сумісність з великою кількістю пристроїв на програмному та апаратному рівні. Для шифрування WPA використовує протокол EAP [2].

3. WPA2 – технологія розроблена у 2004 та є другим поколінням WPA. У цьому поколінні покращили шифрування за допомогою протоколів CCMP та AES. За лік чого була багаторазово підвищена безпека комунікації у бездротовій мережі. У наш час технологія є найбільш популярною та з 2006 року є обов'язковою для сертифікованих приладів Wi-Fi [2].

Покращення безпечної комунікації у бездротових мережах

Здебільшого, організація безпеки бездротової мережі залежить від навичок її власника (адміністратора).

По-перше, варто встановлювати багатосимвольні паролі з використанням малого і великого регістру з додаванням спеціальних символів юнікоду. Це допоможе багаторазово збільшити час брутфорсу (методу грубого перебору паролів).

По-друге, необхідно бути обережним із фішингом. Сучасні набори інструментів, дозволяють блокувати будь-яку точку доступу Wi-Fi та робити її копії, які можуть маскуватися під назвою власника точки доступу але не мають паролю для підключення. В жодному разі не можна вводити свої паролі при підключені та у вебінтерфейсу фейкової точки доступу [3].

Основні види атак на точку доступу

Сучасні зловмисники переважно використовують метод деаутентифікації у комбінації з фішингом чи підбором хеш-суми. Атака методом деаутентифікації відправляє пакети для роз`єднання із точкою доступу одному чи групі її

користувачів. Ця атака може використовуватися для:

- встановлення назви схованої точки доступу;
- нескінченної відправки пакетів деаунтифікації, що приводить до неможливості користування точкою доступу;
- перехвату рукостискань WPA/WPA2;
- генерації ARP запитів [4].

Протокол ARP призначений для ідентифікації MAC-адреси за допомогою IP-адреси іншого комп'ютеру. Він дозволяє пристроям комунікації у локальній мережі робити запит на визначення якому приладу назначена конкретна IP-адреса.

Генерація ARP запитів дозволяє перехоплювати увесь трафік та *cookie*-файли потенціальної жертви за допомогою яких, наприклад, можливо увійти у недавно відвідані соціальні мережі і т.д. Для ефективного захисту від ARP атаки можна зарезервувати IP-адресу за MAC-адресою у відповідному інтерфейсі маршрутизатора. Також, існує програмний захист Ethernet-портів за допомогою функції DAI (функція перевірки підміни пакетів). Вона дозволяє оцінити достовірність кожного ARP-запиту та відкинути зловмисні пакети [4].

Розрахунок часу взлому паролів

Після перехвату рукостискань, зловмисник має підібрати пароль точки доступу за допомогою готових чи згенерованих словників [5].

Для перебору восьми символьного паролю, який складається тільки з цифр необхідно перебрати 10^8 = 100000000 паролів. Якщо використовувати середньостатистичний комп'ютер із дискретною відеокартою, то можливо досягти швидкості перебору понад 400 тис. паролів у секунду. Це означає, що усі восьмисимвольні чисельні паролі можливо зламати лише за 250 секунд. Тому, задля покращення надійності необхідно використовувати багатосимвольні паролі з комбінації чисел, латинських букв малого та великого регістру. Наприклад, для підбору паролю, який складається з двадцяти різних символів зі швидкістю 10 мільйонів паролів у секунду, зловмиснику може знадобиться понад 31 мільйонів років [6].

Список використаних джерел:

1. Що таке Wi-Fi? URL: https://www.newscientist.com/question/what-does-wi-fi-stand-for/
2. Різниця між WEP, WPA, WPA2 алгоритмів безпеки. URL: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
3. Фішинг та безпека у мережі Wi-Fi. URL: https://aircrack-ng.blogspot.com/2020/01/aircrack-ng-16.html
4. ARP запити, використання та захист. Отруєння ARP. URL: https://datatracker.ietf.org/doc/html/rfc2002
5. Метод грубого перебору паролів. URL: https://ieeexplore.ieee.org/abstract/document/8400211
6. Розрахунок надійності паролів. URL: https://www.mecs-press.org/ijcnis/ijcnis-v8-n7/IJCNIS-V8-N7-4.pdf

Науковий керівник: доцент Задерейко О.В.

КІБЕРВІЙНА В УКРАЇНІ

Дикий О.В.

кандидат юридичних наук, доцент
декан факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

У зв'язку з військовою агресією російської федерації проти України 24 лютого 2022 року було введено правовий режим воєнного стану в України. Варто зазначити, що першими були саме масові DDoS-атаки на державні сайти України, банківську систему, ще 23 лютого 2022 року, тобто за день до повномасштабного вторгнення та обстрілів українських міст. Вбачається, що цілю таких кібератак була саме дестабілізація державних та приватних інституцій, вплив на суспільство з метою посіяти панічні настрої.

У війні XXI століття кіберфронт виявися одним із серйозних напрямків активних дій, що безумовно пов’язано із цифровізацією обох сторін війни. Звернемося до дефініції терміну кібервійна. Американський експерт у галузі кібербезпеки Р. Кларк, пропонує так трактування: «Кібервійна – дії однієї національної держави з проникненням у комп'ютери чи мережі іншої національної держави для досягнення цілей завдання шкоди чи руйнування» [1].

Вітчизняний експерт О. Мережко пропонує таке визначення: «Кібервійна – використання Інтернету та пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави» [2].

У Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII складових. Наприклад, кібероборона – це сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

У цьому контексті досить цікаво провести певну аналогію між кібервійною та війною в «реальному» середовищі. Тут хочемо звернути увагу на мобілізаційний потенціал. Так, з моменту вторгнення російської федерації на територію України з перших днів Міністерством цифрової трансформації було створено Telegram канал покликаний масово долучати людей до атак на різні ресурси російської федерації (https://t.me/itarmyofukraine2022). Безумовно він не є ключовим у системній протидії агресору, однак створює серйозні проблеми для противника. Так, за повідомленням із ЗМІ, російські системи постійно стикаються із труднощами функціонування, що дозволяє розпорошувати сили противника на кіберфронті. Вбачається, що в подальшому підготовка мобілізаційного

потенціалу для кіберфронту є однією із пріоритетних. Це пов'язано, в першу чергу, із сучасними умовами ведення війни та їх видозміненням (застосування кібератак). Підготовка таких фахівців повинна здійснюватися для всіх здобувачів освіти в межах галузі знань 12 «Інформаційні технології» у закладах освіти, до того ж до відповідних стандартів освіти повинні бути внесенні відповідні зміни. Як свідчить кількість учасників вказаної групи, до лав кіберармії можна мобілізувати близько 250 тис. осіб (станом на 19.05.2022).

Крім того серед учасників кіберфронту, що стала на захист України після початку повномасштабної війни з росією, об'єдналися наступні групи професіоналів та активістів:

- Досвідчені міжнародні IT-професіонали в галузі кібербезпеки (як представники приватних компаній, так і представники відповідних підрозділів західних спецслужб та підрозділів кібернетичних військ на кшталт британської GIC – Government Information Cell);
- Досвідчені вітчизняні-фахівці в галузі кібербезпеки;
- Українські професіонали в інших галузях IT, що долучилися до кібернетичного фронту як волонтери;
- Існуючі групи фахівців у галузях OSINT (наприклад, Informnapalm) та протидії ворожим дезінформаційним кампаніям (наприклад, StopFake), що сформувалися ще з самого початку агресії Росії у 2014-2015 роках р. та вже зарекомендували себе у боротьбі із ворогом;
- Умотивовані кіберактивісти без спеціальних фахових знань в царині IT, що долучилися до кібернетичного фронту інформаційної війни (поширення правди про події в Україні, участь у пропагандистських кампаніях, розрахованих на населення країни-загарбника, контрпропаганда – боротьба із російськими фейками та дезінформаційними ресурсами в соціальних мережах та в цілому на просторах Інтернету).

Вказане свідчить про значний потенціал саме мобілізаційної складової у активних військових кібердіях.

Також українська сторона використовує краудсорсингові технологій проти ворога на прикладі боту єВорог. Вказаний напрям є одним із новаторських у сучасному світі, так як дозволяє збирати та використовувати інформацію про пересування сил противника фактично в «реальному часі» з детальним описом кількості особового складу та відповідної техніки.

Одним із напрямів кібервійни є протидія пропаганді російської федерації, що направлена на – визначення мародерів армії окупантів через аналіз поштових відправлень та інформування їх родичів через соціальні мережі тощо, а також використання штучного інтелекту для розпізнавання обличчя вбитих солдатів російської федерації та інформування їхніх родичів.

Вказане свідчить про наявний значний напрям подальших наукових досліджень комплексного характеру, що направлений на вивчення феномену

кібервійни, ролі кіберфронту в активних бойових діях та значення мобілізаційного потенціалу кібер фахівців в обороні держави тощо.

Список використаних джерел:

1. Richard A. Clarke and Robert K. Knake»Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010). 2011. 320 p.
2. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). Політичний менеджмент. URL: https://web.archive.org/web/20111007185753/http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.

ЛЮДСЬКИЙ ФАКТОР ЯК ОДИН ІЗ ВИДІВ ВРАЗЛИВОСТЕЙ В КІБЕРБЕЗПЕЦІ

Кравцов О.О.

студент 1-го курсу магістратури
факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Питання про захист інформаційних інфраструктур, є одним з важливих питань для вирішення, як цивільними підприємствами, так і державою в цілому.

Один із аспектів надання якісного захисту інформаційній інфраструктурі являється протистояння внутрішнім загрозам. Будь-яка інформаційна інфраструктура, яка навіть має найновіші програмно-технічні засоби захисту, все ще опрацьовується людиною, що дає злочинцям, дуже велику вразливість, яку вони можуть використовувати для своїх цілей через соціальну інженерію.

Соціальна інженерія – це термін, який використовується для широкого спектру шкідливих дій, що здійснюються через взаємодію людей. Він використовує психологічні маніпуляції, щоб обманом змусити користувачів зробити помилки безпеки або роздати конфіденційну інформацію[1].

Такі вразливості можливо віднести до внутрішніх загроз до інформаційної інфраструктури. Внутрішні загрози – це загрози, що виникають через користувачів із законним доступом до інформаційної інфраструктури.

Такі користувачі використовують цей доступ зловмисно чи ненавмисно для заподіяння шкоди бізнесу. Внутрішні загрози не обов'язково трапляються через працівників підприємства, вони також можуть трапитися через колишніх співробітників, підрядників або партнерів, які мають доступ до систем або даних організації.

Можна виділити 4 внутрішні загрози:

1) Пішаки – це працівники, які маніпулюють зловмисною діяльністю, часто ненавмисно, за допомогою фішингу або соціальної інженерії. Будь то несвідомий працівник, який завантажує зловмисне на свою робочу станцію, або

користувач, який розкриває облікові дані третій стороні, що видає себе за службовця довідкової служби. Одним із прикладів є мережа Ubiquiti Networks, яка була атакована за допомогою фішингу. Електронні листи від вищих керівників змушували працівників перерахувати десятки мільйонів доларів на банківський рахунок дочірньої компанії, зареєстрованої в Гонконзі. Тоді співробітники не знали, що електронні листи підроблені, а банківський рахунок контролюється шахраями.

2) Гуфи – не діють зі зловмисними намірами, а навмисно завдають шкоди. Гуфи – це неосвічені або самовпевнені користувачі, які вважають, що вони звільнені від політики безпеки, незалежно від компетентності. У 95% організацій є працівники, які активно намагаються обійти контроль безпеки, і майже 90% внутрішніх атак спричинені недосвідченими користувачами, які не знають якої шкоди вони можуть завдати своїми діями. Прикладом махінації може бути користувач, який зберігає незашифровану особисту інформацію в обліковому записі хмарного сховища для зручного доступу на своїх пристроях, незважаючи на те, що це суперечить політиці безпеки.

3) Співучасники – це користувачі, які співпрацюють із третьою стороною, часто конкурентами. Такі користувачі використовують їхній доступ таким чином, що навмисно завдають шкоди. Співучасники, як правило, використовують свій доступ для викрадення інтелектуальної власності та інформації про клієнтів або для порушення нормальної ділової діяльності.

4) Самотні вовки повністю незалежні і діють зловмисно без зовнішнього впливу чи маніпуляцій. Такі суб'єкти особливо небезпечні, коли мають підвищений рівень привілеїв, таких як системні адміністратори або адміністратори баз даних. Класичним прикладом самотнього вовка є Едвард Сноуден, який використовував свій доступ до секретних систем для витоку інформації про кібершпигунство в Агентстві національної безпеки США [2].

Список використаних джерел:

1. Social Engineering: URL: https://www.imperva.com/learn/application-security/social-engineering-attack/
2. Andrea GilData: Security – Confidentiality, Integrity & Availability. kVA by UL. URL: https://cutt.ly/4bq5U4G

Науковий керівник: доцент Лобода Ю.Г.

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПЕРЕДАЧІ ТА ОТРИМАННЯ ІНФОРМАЦІЇ У ЗАХИЩЕНОМУ ВИГЛЯДІ

Красношлик О. Ю.

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У наш час інтернет став невід'ємною частиною нашого життя. Він допомагає нам знаходити, обробляти та аналізувати дуже багато інформації. Кожного дня ми дізнаємося щось нове з різних Інтернет-ресурсів, слідкуємо за погодою, новинами, шукаємо інформацію по навчанню чи роботі, спілкуємося з друзями та багато чого іншого.

Технічний прогрес стрімко рухається вперед, всупереч різним умовам, війни та пандемії чи природним явищам. За останнє століття люди зробили величезний технологічний прорив, що вважалося неможливим на початку XX століття, а зараз звичайні для нас речі.

Інтернет зробив величезний внесок у розвиток світу, цивілізації та комфорту людей. Ми можемо спілкуватися через відео з будь-якою точкою планети, де є доступ до мережі Інтернет, ми можемо замовляти їжу онлайн, бронювати квитки на літаки, потяги та автобуси, знаходити швидко відповіді на різні запитання, просто надрукувавши відповідний запит у пошуку.

Згідно з дослідженнями вчених, обсяг інформації, який за день отримує сучасна людина, десь в 10 разів більший, ніж об'єм, який отримували люди XIX століття. Тому, якщо так продовжиться, то ймовірно, кожне наступне покоління буде дедалі розумнішим та розвинутим, ніж попереднє.

Можна сказати, що більшість сучасних дітей вже знають набагато більше інформації та функцій Інтернету, аніж їх дідусі чи бабусі. Це все через те, що їх мозок вже адаптувався до цих технологій, зрозумів як можна ними користуватися на базовому рівні та дізнаватися про нові його можливості.

За Інтернетом – майбутнє. Під час пандемії коронавірусу у 2020-му році більша частина офлайн життя перейшла у режим онлайн.

Тоді майже всі люди на планеті зрозуміли, наскільки важливим є Інтернет та як він може допомогти у подібні моменти у майбутньому.

В цей час, офлайн зустрічі та спілкування також перейшло до онлайну, що викликало небувале зростання кількості користувачів месенджерів, а отже й навантаження на сервери, бази даних та швидкість роботи сервісів спілкування. Почастішали також й хакерські атаки на подібні ресурси, метою яких було отримати доступ до приватних повідомлень людей та порушення захищеності алгоритмів шифрування, які використовуються для створення безпечного та конфіденційного спілкування людей між собою. Тому, безпека подібних ресурсів – пріоритет їх розробників. Сучасні месенджери не завжди точно вказують які

саме алгоритми шифрування вони використовують, тому рівень їх безпеки обміну інформації може бути під сумнівом.

З вищеозначених причин з'явилася ідея створення альтернативного вебресурсу, який буде використовувати модифікований алгоритм шифрування для можливості обміну інформацією. Його актуальність в тому, що під час масштабних збоїв великих сервісів можна буде ним користуватися, щоб не втрачати захищений зв'язок з іншими людьми.

У якості основної мови програмування для цього проекту обрано Python [1]. Його активний розвиток у останні роки дав поштовх для створення сучасних та зручних фреймворків, які допомагають розробнику швидше створювати власні вебресурси. Щоб не «вигадувати велосипед» та не писати однаковий код знову і знову, фреймворки містять у собі спеціальні готові шаблони, бібліотеки та функції. Доповнюючи їх своїми модифікаціями, програміст не витрачає марно час на відтворення того, що вже давно розробили, а приділяє більше часу на реалізацію власних задач.

Яскравим прикладом такого фреймоворку є Django [2]. Його зручний та зрозумілий інтерфейс допомагають швидко орієнтуватися у середовищі. Завдяки цьому фреймворку, мова Python почала широко використовуватися не лише у Data Science, Machine Learning, Big Data та DevOps, але й у Web Development.

Тому й попит на вакансії у цій галузі почав швидко збільшуватися. Бібліотеки Django мають готові рішення не тільки візуальних шаблонів вебсторінок, а ще й власну панель адміністратора, систему парольного захисту та можливість створювати міграції для оновлення таблиць баз даних.

Для створення проєкту та прототипу вебресурсу використовуються СКБД SQLite, яка є доволі простою та зручною у використанні. За допомогою графічного інтерфейсу можна швидко знайти потрібні дані, відстежити чи правильно вони надходять до СКБД [3].

Безпека листування та персональних даних реалізована за допомогою модифікованого алгоритму шифрування Діффі-Геллмана, який буде забезпечувати більш високу криптостійкість та більшу вибірку ключів, що зробить процес дешифрування значно довшим, ніж при оригінальному алгоритмі.

Також, для захисту акаунтів користувачів передбачається використання системи парольного захисту, що здійснює перевірку паролю на складність, наявність обов'язкових великих літер, не менше 8 символів у паролю та запобігання використання найпопулярніших паролів за дослідження компанії NordPass [4].

Для верифікації електронної пошти користувача при його реєстрації буде створений унікальний токен, що надійде на email-адресу. До поки користувач не відкриє цей лист та не перейде за спеціальним посиланням – його акаунт не буде верифікованим та матиме обмежений доступ. Як тільки перехід посиланням відбудеться – сервер обробить перехід за спеціальним токеном, перевірить його валідність. І у разі успішного знаходження – акаунт стає підтвердженим.

Готовий прототип вебресурсу планується розмістити на платформі Heroku для доступу усім користувачам в мережі Інтернет. Дизайн вебресурсу містить патріотичні зображення, щоб його майбутнім користувачам було цікаво та незвично обмінюватися повідомленнями. У разі успішного запуску та підтримки серед суспільства – проект можна розвивати та покращувати.

Список використаних джерел:

1. Python official website. URL: https://www.python.org/
2. Django official website. URL: https://www.djangoproject.com/
3. SQLite. URL: https://sqlite.org/index.html
4. NordPass. Top 200 most common passwords. URL:https://nordpass.com/most-common-passwords-list/

Науковий керівник: доцент Ахмаметьєва Г.В.

ПОБУДОВА МОДЕЛІ СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кухаренко С. В.

кандидат технічних наук, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

У тезах розглядається підхід до структуризації моделі системи забезпечення інформаційної безпеки, який може бути використаний під час моделювання систем захисту інформації.

При побудові сучасних систем забезпечення інформаційної безпеки виникає необхідність дослідження багатьох ситуацій з урахуванням впливу різних випадкових факторів. Тому виникає потреба створення комплексу математичних моделей систем інформаційної безпеки.

Введення пропонованого апарату аналізу систем інформаційної безпеки випливає з необхідності початку формального математичного опису визначених ситуацій при побудові і моделюванні систем захисту.

Об’єктом дослідження є система забезпечення інформаційної безпеки, яка має ієрархічну структуру та безліч складових її об’єктів.

Для спрощення процесу моделювання пропонується надати систему забезпечення інформаційної безпеки у вигляді узагальненої структури.

В узагальненій структурі системи забезпечення інформаційної безпеки на її верхньому рівні можна виділити чотири основні блоки:

1. Блок ресурсів. Він включає доступні системі ресурси - фінансові, технічні, інформаційні.

2. Блок небезпек. Містить базу даних можливих загроз, їх ймовірності та можливості реалізації.

3. Блок параметрів об'єкта. Містить інформацію про фізичну структуру, розташування на місцевості, канали проходження інформації.

4. Блок захисту. Включає використовувані технічні засоби захисту, засоби захисту інформації, організаційні заходи.

Блок системи розподілу ресурсів містить доступні системі ресурси – фінансові, технічні, інформаційні. В цьому блоці необхідно виділити кілька основних підблоків та зв'язків між ними. Це підблоки фінансових ресурсів, людських ресурсів, існуючих технічних засобів захисту, і навіть засобів інформаційного захисту.

Вхідна та вихідна інформація цих підблоків обробляється в блоці обробки, завдання якого - дати відповідь на запит про можливі або необхідні ресурси з урахуванням їх наявності, вартості та сумісності. Цей блок може працювати у двох режимах. По-перше, давати оптимальну інформацію з урахуванням фінансових обмежень та, по-друге, без цих обмежень, але з урахуванням необхідної якості.

Структура блоку загроз передбачає обробку та прогнозування. У ньому обробляється вхідний запит або генерується відповідна загроза або випадковим чином або на основі моделювання відповідної ситуації. У ньому необхідно також врахувати: кримінальні загрози – крадіжки, напади, агресії та ін; природні катаклізми – землетруси, несприятливі погодні умови; внутрішні загрози – неправильні дії персоналу, короткі замикання, зависання комп'ютерів, збої системи захисту; міські загрози – відключення електроенергії, обриви телефонних мереж, затори на дорогах.

Блок параметрів об'єкта визначає фізичну структуру об'єкта, межі безпеки, параметри розмежування доступу, інформаційні потоки на об'єкті. Для правильного опису структури необхідно формалізувати процес розбиття об'єкта на елементарні та локальні зони, межі безпеки. Зіставити фізичним об'єктам (будівлям, поверхам, приміщенням) інформаційні об'єкти (комп'ютери, мережеву структуру, електричні та телефонні мережі), а також систему доступу та переміщення персоналу та відвідувачів на об'єкті. Це завдання можна вирішити з урахуванням інформаційно-фізичної моделі об'єкта, введеної раніше.

Блок системи захисту є центральним блоком загальної моделі системи забезпечення інформаційної безпеки об'єкта. У ньому забезпечується взаємодія решти блоків моделі. Повинні бути передбачені два основні режими роботи – синтез та моделювання системи захисту. По-перше, на основі даних блоку параметрів об'єкта, обмежень, визначених блоком розподілу ресурсів, проектується перший варіант системи захисту об'єкта. На другому етапі дана система захисту піддається впливу загроз, які отримують з блоку загроз. Обчислюється ряд параметрів захищеності об'єкта і порівняється з бажаними. Шляхом варіювання параметрів у блоках розподілу ресурсів та у блоці параметрів об'єкта проводиться пошук оптимального варіанту системи захисту. Для точного аналізу роботи системи захисту необхідне ретельне опрацювання логічної схеми проходження

загрози через межі системи безпеки та апарат аналізу реакції системи захисту на цю загрозу.

Отже, визначивши шляхи вирішення цих завдань, можна суттєво спростити початковий етап побудови систем безпеки.

Список використаних джерел:

1. Грищук Р. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. Грищук, К. Молодецька-Гринчук // *Захист інформації*. 2017. Т. 19, № 4. С. 254-262 URL: http://nbuv.gov.ua/UJRN/Zi_2017_19_4_3.
2. Kahler M. Economic security in an era of globalization. *The Pacific Review*. Vol. 17. No. 4. URL: https://www.tandfonline.com/doi/full/10.1080/09512740 42000326032?scroll=top&needAccess=true
3. Radchenko, S.G. (2015), Formalizovannie i jevristicheskie reshenija v regressionnom analize [Formalized and heuristic solutions in regression analysis], Kornijchuk, Kyiv, Ukraina.
4. Варналій З.С., Онищенко С.В., Маслій О.А. Механізм попередження загроз економічній безпеці України. Економічний часопис XXI. 2016. № 159(5-6). С. 20-24.
5. Системи забезпечення інформаційної безпеки. URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review
6. Економічна безпека підприємств, організацій та установ URL: https://pidru4niki.com/1663080551264/ekonomika/ekonomichna_bezpeka_pidpriyemstv_organizatsiy_ta_ustanov

ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧІВ

Ломановська А. В.

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Одним з важливих завдань є захист даних користувачів від втрати і пошкодження. Це пояснює зростаючий інтерес до способів захисту, які могли б забезпечити безпеку даних користувачів. На даний момент одним з прогресивних напрямків у цій галузі є використання нейронних мереж для вирішення цієї проблеми.

Важливою особливістю нейромереж, яка використовується у сфері забезпечення безпеки даних користувачів, є їх здатність аналізувати складні багаторівневі алгоритми умисних атак на дані користувачів.

Класичним прикладом такого використання є проект STAMINA [1].

STAMINA представляє собою нейромережу яка здатна конвертувати програмний код в монохромне зображення. Надалі зображення піддається аналізу

вбудованими алгоритмами, в результаті якого нейромережа може визначити, чи є файл шкідливим або ж виявити в ньому ознаки зараження. Проект STAMINA був навчений на великому масиві даних, які компанія Microsoft зібрала з допомогою аналізу дистрибутивів, пропущених через антивірус Windows Defender на комп'ютерах мільйонів користувачів. Завдяки цьому нейромережа навчилася виявляти заражені файли, візуально порівнюючи їх з отриманим «зображенням» шкідливого коду.

Антивірус, функціонування якого було засновано на результатах роботи нейромережі STAMINA в 99% випадків виявляє шкідливий програмний код.

Таким чином, застосування нейромережі дозволило організувати [3]:

- виявлення вторгнень;
- виявлення шкідливих дій;
- класифікацію шкідливих дій;
- впровадження навчання програмного забезпечення для захисту від виявлених шкідливих дій;
- оцінку можливих ризиків втрати даних, пов'язаних з функціонуванням самої нейромережі.

Функціонування нейромереж засновано на використанні штучного інтелекту (ШІ), який можна класифікувати за двома рівнями.

ШІ першого рівня широко застосовується в державних і корпоративних структурах. Одним з прикладів цього типу ШІ є пошук і блокування шкідливих програм евристичним методом. ШІ другого рівня являє собою самопрограмоване середовище, яке має особливість до автоматичної модифікації власних алгоритмів через механізм корекції помилок при виробленні рішень. У сфері кібербезпеки його використовують для виявлення різних типів атак і їх попередження.

Застосування нейромереж дозволило значно скоротити час на розпізнавання атак наступних типів:

1. *DDos* - атак, які зводяться до генерації надлишкового трафіку від хоста, з-за чого відбувається перенавантаження обслуговуючого сервера і послідуюче його відключення.
2. *R2L* – невідомий користувач отримує управління комп'ютером віддалено;
3. *Probe* – отримання конфіденційної інформації за допомогою сканування портів;
4. *U2R* – отримання зареєстрованим користувачем прав суперкористувача (root);
5. *Main-in-the-Middle* – перехоплення даних, з допомогою якого можна впроваджуватися в існуюче підключення;
6. *Session Hijacking* – один з варіантів Main-in-the-Middle, який дозволяє втручатися у відкритий канал передачі даних, для отримання доступу до інформації або до служб у комп'ютерній системі.

Проведені дослідження на виявлення нейромережею перших чотирьох атак показало, що вони можуть успішно справлятися з визначенням цих атак з великою точністю. Для виявлення п'ятого і шостого типів атак застосовувалися рекурентні нейронні мережі, які орієнтовані на обробку послідовних значень.

Таким чином, можна з упевненістю стверджувати, що дослідження в області захисту даних користувачів з використанням нейронних мереж відкрили перспективні можливості для використання їх у сфері кібербезпеки.

Список використаних джерел:

1. Нейромережа STAMINA. URL: https://www.iguides.ru/main/security/microsoft_i_intel_sozdayut_idealnyy_antivirus/.
2. Штучний інтелектURL: https://spydell.livejournal.com/633585.html.
3. Нейромережі в кібербезпеки. URL: https://habr.com/ru/post/587694/

Науковий керівник: доцент Задерейко О.В.

МЕТОДИ ЗАХИСТУ БАЗ ДАНИХ

Маскименко А.С.

студентка 1 курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Сучасні компанії обов’язково мають свою особисту конфіденційну інформацію різних видів, яку треба забезпечити максимальну безпеку в середовищі бази даних.

База даних (БД) – це впорядкований набір логічно взаємопов’язаних даних або сукупність матеріалів, які можуть бути найдені і оброблені за допомогою комп’ютера. БД використовується спільно, та призначена для задоволення інформаційних потреб користувачів.

Система керування базами даних (СКБД) - це комплекс програмних і мовних засобів, необхідних для створення баз даних, підтримання їх в актуальному стані та організації пошуку в них необхідної інформації.

Головним завданням БД є збереження значних обсягів інформації (даних).

На сьогоднішній день існують такі аспекти захисту інформації [1]:

- цілісність;
- захист інформації від несанкціонованої модифікації;
- конфіденційність;
- захист від несанкціонованого ознайомлення з інформацією;
- доступність в сенсі підтримання системи в робочому стані та способи швидко відновити втрачену чи пошкоджену інформацію.

Відповідно, до даних аспектів захисту інформації, виділяють такі загрози:

- загрози цілісності (знищення та модифікація інформації);

- загрози доступності (блокування та знищення інформації);
- загрози конфіденційності (несанкціонований доступ, витік та розголошення інформації).

Безпека баз даних – це комплекс організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації (в тому числі від незаконного використання та шкідливих загроз та атак).

Методи захисту баз даних в СКБД

Захист надійним паролем [2]. Надійність пароля є мірою ефективності від його вгадування або брутфорс атак. У своїй звичайній формі, він оцінює, скільки спроб зловмисникові, не маючи прямого доступу до пароля, потрібно, в середньому, щоб правильно вгадати його. Сила пароля – це функція, що враховує довжину, складність і непередбачуваність. Захист паролем – є самим простим способом захисту БД від несанкціонованого доступу. Паролі можуть бути встановленні користувачами або адміністраторами. Їх облік і зберігання виконується СКБД. Паролі зберігаються в спеціальних файлах СКБД в зашифрованому вигляді. Після введення пароля користувачу надається доступ до необхідної інформації. Не дивлячись на простоту парольного захисту, він має ряд недоліків. По-перше, пароль є вразливим, особливо якщо він не шифрується при зберіганні в СКБД. По-друге, користувачу потрібно запам'ятати або записати пароль, а при недбалому відношенні до запису пароль може стати надбанням інших.

Наявність резервних копій. Ефективним способом для запобігання втраті інформації може бути фіксація всіх копій і БД. Під час виконання резервного копіювання інформації для врахування всіх критично важливих даних треба провести попередню інвентаризацію. Не всі дані є критично важливими або потребують захисту, тому на них немає сенсу витрачати час і ресурси.

Шифрування [3]. Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації. Кращий спосіб захистити базу даних – зашифрувати зробити прочитання неможливим для осіб, що не володіють ключами шифрування. Важливою особливістю будь-якого алгоритму шифрування є використання ключа, який стверджує вибір якогось конкретного методу кодування із всіх можливих. Розрізняють два основні методи шифрування: симетричне й асиметричне. В симетричному шифруванні один і той же ключ використовується і для шифрування, і для дешифрування. В асиметричних методах застосовуються два ключі. Один з них, несекретний, використовується для шифрування і може публікуватися разом з адресою користувача, другий, секретний, застосовується для дешифрування і відомий тільки одержувачу. Шифрування забезпечує всі три аспекти безпеки даних: конфіденційність, цілісність і доступність.

Розділення прав доступу до об'єктів БД. Треба організовувати обмеження дозволів та привілеїв. Власник об'єкта, а також адміністратор БД мають всі права. Решта користувачів мають ті права і рівні доступу до об'єктів, якими їх наділили. Дозвіл на доступ до конкретних об'єктів бази даних зберігається в файлі робочої

групи. Файл робочої групи містить дані про користувачів групи і зчитується під час запуску. Файл зберігає наступну інформацію: імена облікових записів користувачів, паролі користувачів, імена груп, в які входять користувачі.

Для розділення прав доступу до об'єктів БД слід застосувати:

- обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією;
- обмеження використання основних процедур тільки певними користувачами;
- уникнення використання і доступу до баз даних у не робочий час.

Захист полів і записів таблиць БД. Так як у комп'ютерній базі даних вся інформація подається у таблиці, то захист полів і контенту таблиць є ключовим аспектом захисту інформації.

Забезпечення цілісності зв'язків таблиць. Всі таблиці БД мають кореляційні зв'язки, тому будь-яке мінімальне несанкціоноване втручання може мати великі негативні наслідки.

Базу даних слід розміщувати на сервері, недоступному безпосередньо через мережу Інтернет, щоб запобігти віддаленому доступу зловмисників до корпоративної інформації. Важливе значення також має фізична безпека сервера баз даних та резервного обладнання від крадіжок та стихійних лих.

Безпечне використання застосунків. Деякі застосунки містять вразливості, що піддаються атакам. Вразливості та ризики, пов'язані з конфіденційністю, можуть використовуватися зловмисниками для отримання несанкціонованого доступу до інформаційних ресурсів організації або даних користувача. Вразливі застосунки ініціюють з'єднання з мережею, іншими застосунками або сторонніми сервісами, що робить необачного користувача більш вразливим до атаки зловмисників.

Оновлення системи та зміна налаштувань за замовчуванням. Рекомендується також вимкнути всі служби і процедури, які не використовуються.

Вбудовані засоби контролю даних. Вони є доступними але не завжди можуть повністю вирішити виникаючі на практиці проблеми. Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби.

Організація спільного використання об'єктів БД в мережі. Сьогодні проблема доступу користувачів до віддалених баз даних, може вирішуватися за допомогою створення та використання локальних і глобальних мереж передачі даних, а також надання відповідного доступу до баз даних користувачам. База даних може бути локальною, коли користувач підключається до неї безпосередньо, і віддаленою - у випадку підключення до неї на великій відстані. Підключення до віддаленої бази даних здійснюється за допомогою мережевого забезпечення та відповідних протоколів передачі даних. Слід зазначити, що

використання Web-технології для доступу до БД має забезпечити надійний захист інформаційних потоків. Це досягається створенням брандмауерів - апаратно-програмних систем міжмережевого захисту від несанкціонованого доступу до сервера БД.

Процедури ідентифікації, автентифікації і авторизації в СКБД [4]. Сутність процедури ідентифікації полягає в призначенні користувачу БД – імені. Ім'я користувача – це деяка унікальна мітка, що відповідає прийнятим угодам і забезпечує однозначну ідентифікацію об'єкта реального світу в просторі об'єктів, що відображаються. Сутність процедури автентифікації полягає в підтвердженні автентичності користувача, що представив ідентифікатор. У ряді сучасних СКБД використовується:

- біометрична автентифікація - це процес доведення і перевірки автентичності заявленого користувачем імені через пред'явлення користувачем своїх біометричних характеристик (наприклад, відбитки пальців і долоні, звуки голосу, обличчя, відбиток сітківки ока, особливості роботи на клавіатурі, електронний цифровий підпис);
- парольна автентифікація - це процес доведення і перевірки автентичності заявленого користувачем імені шляхом введення ним пароля або парольної фрази. Парольні фрази забезпечують більшу безпеку, ніж короткі паролі, але вимагають більшого часу для введення. Заходами, що дають змогу підвищити надійність парольного захисту є: накладання технічних обмежень, управління терміном дії паролів, обмеження доступу до файлу паролів, обмеження кількості невдалих спроб входу в систему, використання програмних генераторів паролів;
- автентифікація із застосуванням токенів. Токен - це предмет або пристрій, володіння яким підтверджує автентичність користувача.

Переведення непродуктивних баз даних в анонімні [5]. Багато компаній інвестують час та ресурси у захист своїх продуктивних баз даних, але при розробці проекту або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію. За допомогою маскування та анонімізації можна створити аналогічну версію з тією ж структурою, що і оригінал, але із зміненими конфіденційними даними для їх захисту. За допомогою цієї технології значення змінюються за умови збереження формату. Дані можуть бути змінені шляхом змішування, шифрування, переставляння символів або заміни слів. Конкретний метод, правила і формати, залежать від вибору адміністратора, але незалежно від вибору, метод повинен забезпечити неможливість отримати вихідні дані за допомогою зворотної інженерії. Цей метод рекомендовано використовувати для баз даних, які є частиною середовища тестування і розробки, оскільки він дозволяє зберегти логічну структуру даних, забезпечуючи відсутність доступу до конфіденційної інформації поза виробничим середовищем.

Проведення моніторингу активності БД. Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким. Володіння повною історією транзакцій дозволяє зрозуміти шаблони доступу до даних і модифікацій і, таким чином, допомагає уникати витоку інформації, контролювати небезпечні зміни і виявляти підозрілу активність в режимі реального часу.

Перегляд існуючої системи на предмет будь-яких відомих або невідомих уразливостей та визначення та реалізація дорожньої карти/плану їх зменшення.

Можна зробити висновок що використання лише якогось певного методу не може гарантувати повного зберігання даних. Тому для підвищення рівня безпеки інформації в БД рекомендовано використання комплексних заходів.

Розробки в сфері безпеки БД є дуже актуальними та потребують майже не щоденного вдосконалення.

Особливої актуальності ця проблема набула в час російсько-української війни, коли задля безпеки на рівні держави вжили максимальних заходів - закрили повний доступ для всіх державних реєстрів, тим самим відсікли їх від глобальної мережі.

Список використаних джерел:

1. Касянчук, Н. В., Ткачук Л. М. Захист інформації в базах даних. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/7001/5715. 2019
2. Як створити надійний пароль — рекомендації спеціалістів ESET. URL: https://eset.ua/ua/news/view/649/nadezhnyy-parol-sposoby-sozdaniya-parolya- ot-spetsialistov-eset
3. Шифрування та захист баз даних. URL: https://iitd.com.ua/shifruvannj a-ta-zahist-baz-danih/
4. Системи управління базами даних. URL: http: //rodak.if. ua/komptech/lection4 .htm
5. Защита баз данных – залог безопасности корпоративной сети. URL: https: //eset.ua/ua/blog/view/14/

Науковий керівник: доцент Задерейко О.В.

ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Максимчук А.Ю.

студентка 1 курсу судово-адміністративного факультету факультету Національного університету «Одеська юридична академія»

Сьогодні інтернет всюди проник у наше життя і діяльність. Користувачі використовують його кожен день, починаючи з соціальних мереж і до онлайн-банкінгу. Також цей ресурс який використовується для навчання і праці.

Сучасні користувачі мають доступ до інтернету майже з усіх власних електронних приладів: комп'ютери, смартфони, планшети, телевізори тощо.

Саме цей факт обумовлює необхідність знань про безпеку в мережі Інтернет [1].

Кожен користувач має віднайти для себе оптимальні засоби захисту своїх персональних даних, щоб в подальшому житті їх не могли використовувати зловмисники.

До персональних даних може бути віднесені не тільки ім'я прізвище чи дата народження. У законодавстві України так називають будь-яку інформацію яка допомагає ідентифікувати особистість користувача. Тобто персональними даними можуть бути:

- ім'я та прізвище;
- дата та місце народження;
- сімейний стан;
- паспортні дані;
- професія тощо.

Також варто зазначити, що паролі та акаунти не являються персональними даними, бо вони не несуть конкретну інформацію про особу. Але можуть бути використаний злочинцями для здобуття важливої інформації.

Захист особистих даних

Пересічному користувачеві мережі Інтернет рекомендовано наступні кілька способів збереження персональної інформації [2]:

1. Створення складних паролів. Він має містить в собі букви цифри, великі й малі, не менше ніж 12 символів. А також важливо, що пароль не містив особливих даних таких як: прізвище або дата народження.

2. Оновлення програмного забезпечення. Необхідно своєчасно оновлювати програмне забезпечення навпаки, Адже розробники ретельно слідкують за наявністю можливих загроз і намагаються захистити свій продукт.

3. Використання двофакторної аутентифікації. Найбільш дієвий критерій в для захисту даних. Різні мережеві сервіси мають можливість підтвердження двофакторної автентифікації. Частіше це робиться за допомогою СМС повідомлення. Але існує можливість його перехоплення. Замість СМС краще спробувати такі застосунки як Google Authenticator.

4. Правила користування публічним Wi-Fi. В суспільних місцях, необхідно користуватися VPN-з’єднанням.

5. Спостереження за адресним рядком. Необхідно слідкувати за наявністю безпечного з’єднання підчас web-серфінгу. Безпечніше, щоб web-браузер використовував HTTPS з’єднання.

6. Конфіденційність у соцмережах. При користуванні соціальними мережами необхідно пам'ятати, що будь-яка інформація, яку користувач вирішив оприлюднити у себе на сторінці, автоматично стає загальнодоступною.

Справа в тому, що кожна соцмережа є безцінним джерелом інформації для зловмисників, які збирають персональні дані, які вони потім використовують для обману і шахрайства. Тому дуже важливо правильно налаштувати конфіденційність профілю користувача будь-яких соцмережах.

7. Захищеність електронної Пошти. Як правило в електронній поштовій скриньці зберігаються "ключі" від більшості облікових записів користувача, так як процедура відновлення пароля найчастіше здійснюється саме за допомогою email-повідомлень. Тому життєво необхідно захистити свою основну поштову скриньку, до якої прив'язані інтернет-банк і найважливіші мережеві сервіси. Якщо користувач бажає зареєструватися на сайті знайомств або в якомусь сумнівному сервісі, краще створити запасну поштову скриньку.

В статті 24 Закону України "Про захист персональних даних" вказано що "Власники, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкової втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних" [3]. Тобто, по-перше, користувачі самі несуть відповідальність за збереження їх персональних даних.

Отже, якщо користувач будете дотримуватись вказаних вимог тоді його персональні дані будуть більш захищеними.

Список використаних джерел:

1. Безпека в Інтернеті, що потрібно знати. URL: https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html
2. 5 шляхів захисту особистих даних в Інтернеті. URL: https://beetroot.academy/blog/general/5-shlyahiv-zahistu-osobistih-danih-v-interneti
3. Законодавство України. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/en/2297-17#Text

Науковий керівник: доцент Задерейко О.В.

АНАЛІЗ АКТИВНОСТІ КОРИСТУВАЧА ЗА ПРОФІЛЕМ БРАУЗЕРА CHROME

Малюта В. В.

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Років 20 тому, коли Інтернет з долі обраних почав стрімко перетворюватися в масове явище, перед тисячами новоспечених користувачів виникло питання: яку пошукову систему використовувати?

Тепер ми користуємося улюбленої пошуковою системою швидше в силу звички, не замислюючись про те, що від вибору пошуковика залежить комфорт користувача, його конфіденційність і якість пошукової видачі.

Веббраузер доставить вас в будь-яке місце в Інтернеті, дозволяючи переглядати текст, зображення і відео з будь-якої точки світу. Інтернет – це величезний і потужний інструмент. Протягом декількох десятиліть Інтернет змінив те, як ми працюємо, як ми граємо і як ми взаємодіємо один з одним.

Залежно від того, як він використовується, він пов'язує нації, стимулює торгівлю, розвиває відносини, стимулює інноваційний двигун майбутнього.

Важливо, щоб у всіх був доступ до мережі, але також важливо, щоб ми всі розуміли, які інструменти ми використовуємо для доступу до неї. Ми використовуємо веббраузери, такі як Mozilla Firefox, Google Chrome, Microsoft Edge і Apple Safari, кожен день, але чи розуміємо ми, що це таке і як вони працюють? За короткий проміжок часу ми перестали дивуватися здатності відправляти електронні листи кому-небудь по всьому світу і змінили наше уявлення про інформацію. Питання в тому, який браузер або додаток може допомогти вам швидше отримати інформацію.

Останнім часом користувачі все частіше почали звертати увагу на те, які саме дані про них збирають у застосунках та на вебсайтах. Саме тому великі корпорації намагаються робити систему збору інформації більш прозорою для звичайних користувачів. Зокрема, компанія Google впровадила нову функцію, завдяки якій за декілька простих кроків можна налаштувати конфіденційність власних даних [1].

Користуючись Інтернетом, ви напевно багато разів помічали такі «збіги»: зайдете на сайт автосалону, а потім вам всюди показують рекламу машин. Або після відвідування сайту для батьків вас починає переслідувати реклама підгузків і дитячих сумішей.

Все це можливо тому, що найбільші рекламні мережі і безліч інших інтернет-сервісів по збору інформації («брокери даних») намагаються скласти максимально повний портрет кожного інтернет-користувача на основі всіляких – і часто відкритих – даних. Зазвичай це у них виходить. В інтернеті за вами може стежити хто завгодно – як законними способами, так і з порушенням прав на захист особистої інформації. Від одних способів стеження захиститися важко, від інших – потрібно. Але навіть озброївшись усіма засобами для протидії, пам'ятайте: гарантовано уникнути інтернет-стеження можна лише якщо фізично відключилися від доступу до інтернету. Але і то не факт.

Як боротися? Користуватися новітніми версіями браузерів. Chrome, анонсував і впровадив низку функцій для боротьби зі стеженням [2].

Радикальне рішення – відключити Javascript, мову, яка використовується для збору даних; але більшість сайтів тоді відразу «зламаються». Можна спробувати «пересісти» на найпопулярніший смартфон-планшет-ноутбук у відповідному регіоні і не персоналізувати налаштування.

Список використаних джерел:

1. Steve Rura/ A fresh take on an icon/ Google Inc.
2. Julia Angwin / Sun Valley: Schmidt Didn't Want to Build Chrome Initially, He Says. *WSJ Digits Blog*.

Науковий керівник: доцент Ахмаметьєва Г.В.

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ НАД РОЗШИРЕНИМ ПОЛЕМ $GF(2^m)$ ЕЛІПТИЧНИХ КРИВИХ

Онацький О. В.

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Жарова О. В.

кандидат фізико-математичних наук, доцент кафедри вищої математики Національного університету «Одеська політехніка»

В роботі запропоновано протокол автентифікації з нульовим розголошенням (zero-knowledge) на основі математичного апарату еліптичних кривих (elliptic curves – EC) з використанням особистих даних користувача та секретних ключів абонентів. Безпека криптосистем на еліптичних кривих (elliptic curves cryptography) [1], заснована на труднощах розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої (elliptic curve discrete logarithm problem) [2]. У криптосистем на EC запропоновано використовувати криптоперетворення, що базуються на перетвореннях у групі точок еліптичних кривих над полями $GF(p)$, $GF(2^m)$, $GF(p^m)$ [1, 2].

У криптосистемах над розширеним полем $GF(2^m)$ рівняння EC має вигляд [1, 2]:

$$y^2 + xy \equiv (x^3 + ax^2 + b) \bmod (f(x), 2) \text{ – несуперсингулярна крива;}$$

$$y^2 + cy \equiv (x^3 + ax + b) \bmod (f(x), 2) \text{ – суперсингулярна крива,}$$

де x, y – точки EC, $x, y \in E(GF(2^m))$; a, b, c – коефіцієнти EC; $f(x)$ – незведений поліном над полем $GF(2)$ вигляду

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \ldots + h_{m-1} x^1 + h_m,$$

причому $h_i \in GF(2)$.

Визначимо над точками з $E(GF(2^m))$ операцію складання та подвоєння. Нехай відомі координати двох точок $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то сума $P + Q = (x_3, y_3)$ визначається згідно з правилами [1, 2]:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + x_1 + x_2 + a) \bmod (f(x), 2);$$

$$y_3 \equiv [\lambda(x_1 + x_3) + x_3 + y_1] \bmod (f(x), 2);$$

2) суперсингулярна крива

$$x_3 \equiv (\lambda^2 + x_1 + x_2) \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2),$$

де $\lambda \equiv \left(\frac{y_1 + y_2}{x_1 + x_2} \right) \bmod (f(x), 2)$.

Точка, що подвоєна $2P = 2(x_1, y_1) = (x_3, y_3)$, визначається згідно з правилами:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + a) \bmod (f(x), 2);$$
$$y_3 \equiv [x_1^2 + (\lambda + 1)x_3] \bmod (f(x), 2),$$

де $\lambda \equiv \left(x_1 + \frac{y_1}{x_1} \right) \bmod (f(x), 2)$.

2) суперсингулярна крива

$$x_3 \equiv \lambda^2 \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2),$$

де $\lambda \equiv \left(\frac{x_1^2 + a}{c} \right) \bmod (f(x), 2)$.

Усі параметри є поліномами не вище m-степеня, а $f(x)$ – примітивний поліном над полем $GF(2)$.

Нехай $E_p(a, b)$ – еліптична крива, відома учасникам інформаційного процесу; $f(x)$ – незведений поліном над полем $GF(2)$; G – попередньо погоджена точка цієї кривої; $\#E_p(a, b) = n$ – порядок групи кривої; M – особисті дані абонента A; k_a і k_b – секретні ключі абонентів A, B; $h(MG) = m$ – геш-функція.

Абонент A обчислює значення відкритого ключа $Y_a = k_aG \bmod (f(x), 2)$ та заявку $\gamma = rG \bmod (f(x), 2)$, які передає абоненту B. Абонент B обчислює значення відкритого ключа $Y_b = k_bG \bmod (f(x), 2)$, який передає абоненту A. Абонент A обчислює два значення $x_1 = [k_aY_b + MG] \bmod (f(x), 2)$ і $x_2 = [(k_a + r)Y_b] \bmod (f(x), 2)$, які передає абоненту B. Абонент B перевіряє рівності: $MG = [x_1 - k_bY_a] \bmod (f(x), 2)$, $h(MG) = m$ та $k_b\gamma = [x_2 - k_bY_a] \bmod (f(x), 2)$.

Для аналізу та перевірки запропонованого протоколу автентифікації на стійкість до атак противника був застосований програмний продукт AVISPA [3]. В роботі виконано перевірку моделі запропонованого протоколу (рис. 1) та результат моделювання зловмисника на протокол представлено на рис. 2.

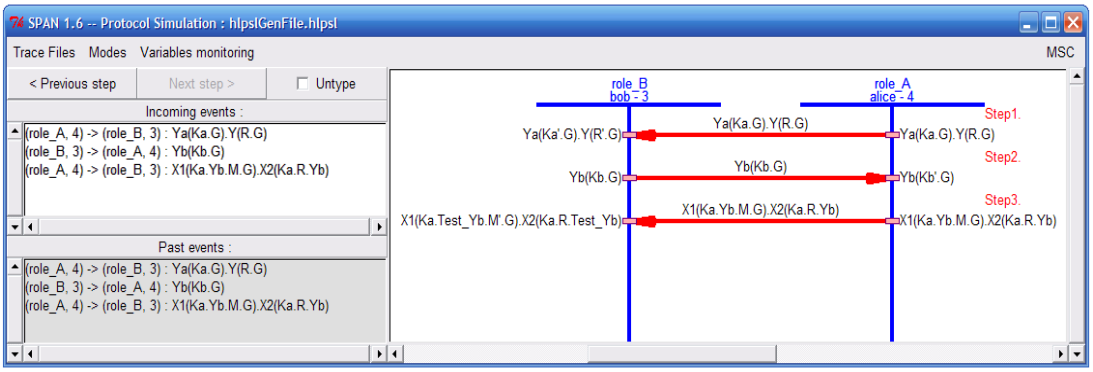


Рис. 1. Перевірка моделі криптографічного протоколу автентифікації

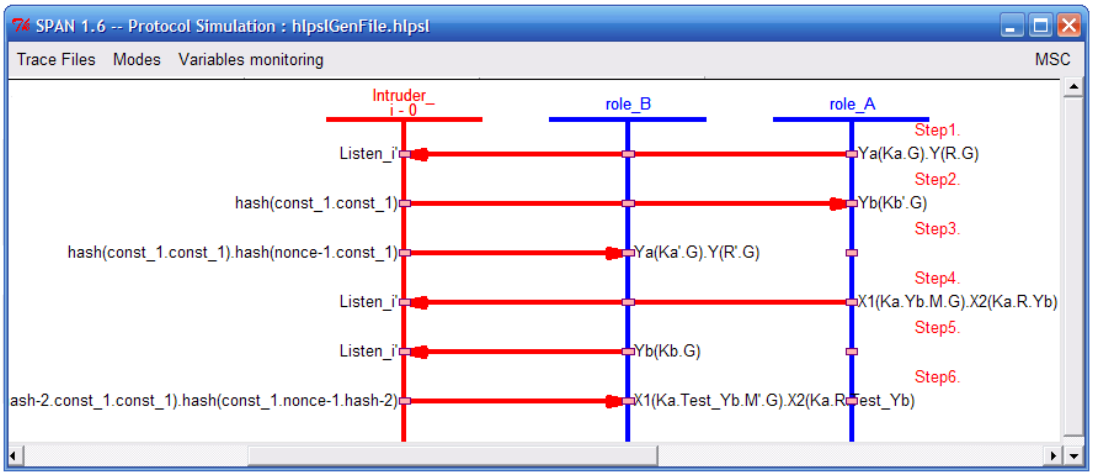


Рис. 2. Результат моделювання дії зловмисника на протокол автентифікації

Програмна верифікація протоколу і стійкість протоколу до атак зловмисника була виконана за допомогою програмних модулів OFMC та CLAtSe AVISPA. В результаті перевірки запропонованого протоколу автентифікації відомих атак не знайдено (рис. 3).

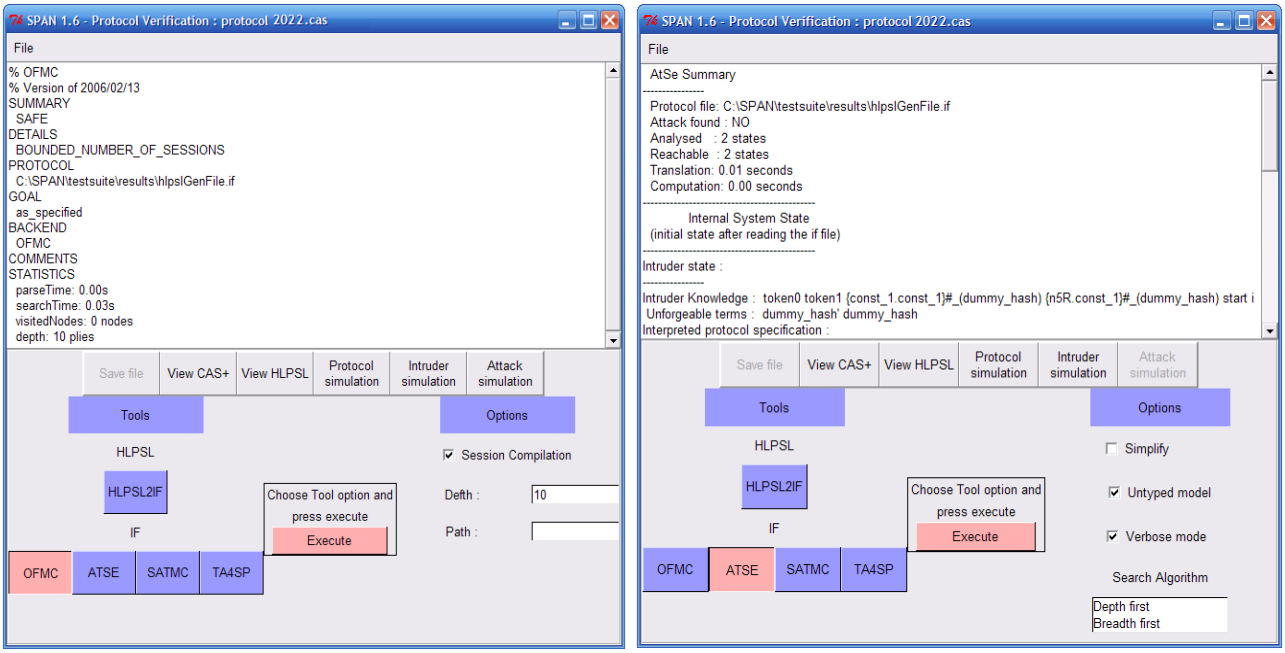


Рис. 3. Верифікація і стійкість протоколу автентифікації до атак

Таким чином, у роботі запропоновано новий криптографічний протокол автентифікації з нульовим розголошенням на основі математичного апарату еліптичних кривих над розширеним полем $GF(2^m)$. Визначено повнота і коректність протоколу, була виконана перевірка моделі і верифікація протоколу. В результаті перевірки протоколу відомих атак на протокол, не знайдено. Для реалізації запропонованого протоколу автентифікації можна використовувати рекомендовані еліптичні криві згідно FIPS 186-4 [4], SEC 2 [4] та ДСТУ 4145-2002 [6].

Список використаних джерел:

1. Stavroulakis P., Stamp M. Handbook of Information and Communication Security: Berlin: Springer-Verlag, 2010. 863 p.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія, Харків: Видавництво «Форт», 2012. 880 с.
3. AVISPA. URL: http://www.avispa-project.org/
4. FIPS 186-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
5. SEC 2. URL: https://www.secg.org/SEC2-Ver-1.0.pdf
6. ДСТУ 4145-2002. URL: https://ru.wikipedia.org/wiki/ДСТУ_4145-2002

СУЧАСНІ СИСТЕМИ ПОЖЕЖНОЇ БЕЗПЕКИ

Раєв О. Д.

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Засоби новітньої протипожежної сигналізації – це є, зокрема, сукупністю технічних засобів, які винайдено для пожежовиявлення, а також обробки зібраної інформації та її передачі, наприклад, у вигляді сповіщення про займання у приміщенні, а також підключення команд автоматичних установок для системи захисту проти диму, їхнього технічного та інженерного наповнення [1].

Бездротова пожежна сигналізація є одним із актуальних для сьогодення видів охоронних систем, які використовуються під час організації захисту об'єктів від пожежі. Сфера їхнього застосування і пристосування досить широка, її ефективність ґрунтується на можливості вести роботу в діалоговому режимі та використовувати резервні станції зв'язку.

Бездротова пожежна сигналізація створена вирішувати цілий комплекс завдань із забезпечення безпеки об'єкту, таких як:

1) постійне сканування контрольованого об'єкта;

2) фіксація параметрів пожежі: температура, задимленість, електромагнітне випромінювання, порівняння отриманих даних із граничними значеннями, занесеними на згадку про приймально-контрольний пристрій;

3) виявлення осередку займання на ранніх стадіях;

4) формування та пересилання тривожного сигналу на одну із зазначених у пам'яті системи адрес: центральний диспетчерський пульт; віддалений пульт управління оператора пожежної охорони; телефонний номер власника об'єкта чи відповідальної особи;

5) активація засобів оповіщення та системи евакуації;

6) активація засобів автоматичного пожежогасіння.

Переваги та недоліки бездротових систем пожежної сигналізації.

Переваги:

1) Установка приладу може виконатись тільки після закінчення оздоблювальних робіт у приміщенні, оскільки не потрібно «штробування» стін для прихованої прокладки кабелів;

2) Система має простішу і водночас гнучку конфігурацію системи;

3) Усуваються фінансові витрати на кабель, вартість самого монтажу суттєво нижча за середньо-статичну ринкову, час виконання робіт значно знижується;

4) Надійна робота системи загалом: відсутність поломок, пов'язаних із втратою контакту або пошкодженнями шлейфів, особливо під час пожежі, що дає змогу відстежувати реальну ситуацію розповсюдження вогню у будівлі.

Недоліки:

1) Незважаючи на прикметний захист, фіксуються помилкові спрацьовування електромагнітних полів працюючого обладнання;

2) Використання бездротових систем в будівлях основних несучих і огороджувальних конструкцій, які виконано із залізобетону або металу, обмежено через «екрануючий» ефект;

3) Для деяких пристроїв стеження та оповіщення необхідні джерела живлення, що обмежує їхнє місце розташування;

4) Необхідний моніторинг рівня заряду автономних джерел живлення для сповіщувачів.

В даний час набули широкого поширення різні «самозбірні» системи, що реалізують на базовому рівні функціонал промислових систем. При цьому розробка, розгортання та експлуатація таких систем найчастіше ефективніша, оптимальніша і економніша по всій сукупності показників, ніж готових промислових рішень. Найпоширенішим рішенням таких систем є платформа Arduino. З урахуванням перелічених вище недоліків та переваг систем бездротової пожежної сигналізації є перспективним створення, реалізація та експлуатація системи бездротової сигналізації на даній платформі. Наявність готових компонентів у вигляді GSM-модуля, датчиків виявлення загоряння дозволить суттєво оптимізувати вирішення цього завдання.

Список використаних джерел:

1. Система пожежної сигналізації. URL: http://florian101.com/services/montazh-p%D1%96dtrimannya-ekspluatats%D1%96i-sistem-pozhezhnoi-signal%D1%96zats%D1%96i
2. Види пожежної сигналізації. URL: https://ohorona-kyiv.com/ua/blog/vidy-pozharnoj-signalizacii.html

Науковий керівник: доцент Бойко В. Д.

РОЗГОРТАННЯ СИСТЕМИ РАННЬОГО ВИЯВЛЕННЯ ПОЖЕЖІ З ВИКОРИСТАННЯМ ПЛАТФОРМИ АРДУЇНО

Соловйов А. С.

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Для боротьби із займанням велике значення мають сучасні пристрої раннього выявленная диму. Кожне місце, де можуть знаходитись пристрої збереження електронної інформації, повинні бути обладнані датчиками сповіщення про пожежу. Для якісного захисту від займання, необхідно правильно організувати заходи щодо пожежної безпеки.

Найбільше використовуються такі типи датчиків раннього виявлення диму:

1. Дротові.
2. Бездротові.

Дротові датчики диму бувають іонізаційні та фотоелектроні.

Іонізаційні пристрої – мають складній дизайн, складаються вони з камери, радіоактивного іонізуючого повітря матеріалу [1]. Фотоелектроні – ці сповіщувачі розроблені за принципом розсіювання світла, таким чином коли дим від вогню змінює інтенсивність світла на кристал, тоді цей датчик й повідомляє про задимлення або пожежу.

Основними недоліками дротових датчиків сповіщення виступають:

- система встановлення датчиків повинна бути розроблена, но етапі планування будівлі;
- не працюють при вимкненій електромережі.

Бездротові датчики диму бувають з температурними та газовими сенсорами. Прикладами бездротових систем раннього сповіщення про пожежу будуть виступати «Ajax» «FireProtect» та «Perenio» PECSS01. Ці 2 датчики маюсь схожий принцип роботи, для коректної та більш функціональної роботи вони мають буди підключені до головного пристрою «Хабу». Якщо у приміщенні у якому розтасований датчик диму, у повітрі з'являються частки диму, датчик відправляє дані до хабу. Хаб у свою чергу за лічені секунди обробляє отримані дані з датчиків і приймає рішення, якщо показники які отримав датчик перевищують норму у 1000 PPM («parts per million» – тобто, частинок на мільйон), то хаб вмикає звукові сповіщувачі, та відправляє повідомлення у фірмовий додаток [2, 3].

Недоліки «Ajax» «FireProtect»:

- потреба мати головний хаб;
- потреба мобільного застосунку для налаштування;
- система повинна бути постійно приєднана до мережі Інтернет («Хаб» та мобільний додаток);
- висока вартість усієї системи.

Недоліки «Perenio» PECSS01:

- необхідне постійне підключення до мережі Інтернет;
- потреба у мобільному застосунку для налаштування;
- повідомлення приходить лише у додаток.

У даному докладі пропнується датчик диму на основі мікроконтролеру «Arduino Leonardo», який дозволяє уникнути перелічених недоліків та використовує наступні апаратні модулі:

- мікроконтролер «Arduino Leonardo»;
- датчик диму «MQ-2»;
- GSM модуль «SW M590E»;
- датчик звукового сповіщення «MH-FMD»;
- акумуляторна батарея.

Датчик диму на мікроконтролері «Arduino Leonardo» працює на основі газового сенсора «MQ-2», який при виявлені часток диму відправляє сигнал до мікроконтролер, якщо цей сигнал перевищує норму у 1000 PPM, «Arduino Leonardo» завдяки алгоритму увімкне звуковий сповіщувач та відправить SMS повідомлення на задані у алгоритмі номери телефону.

Переваги запропонованого рішення :

- датчик не потребує Інтернет-з'єднання;
- не потрібний мобільний додаток для його налаштування;
- можна працювати з будь яким типом мобільного пристрою (телефону);
- надійність приладу і системи;
- низьке електроспоживання пристрою.

Список використаних джерел:

1. WorldVision. URL: https://worldvision.com.ua/v-chem-raznitsa-mezhdu-ionizatsionnymi-i-fotoelektricheskimi-pozharnymi-datchikami/
2. Ajax. URL: https://ajax.systems/ru-ua/products/fireprotect/
3. Perenio. URL: https://perenio.ua/ru/catalog/datchik-dyma-pecss01-pecss01

Науковий керівник: доцент Бойко В. Д.

ЩОДО ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ, ЩО ЗБЕРІГАЄТЬСЯ НА КОМП'ЮТЕРАХ КОРИСТУВАЧІВ

Чанишев Р. І.

кандидат юридичних наук, доцент,
доцент кафедри інформаційних технологій,
Національного університету «Одеська юридична академія»

Незважаючи на всі заходи, що вживаються фахівцями із забезпечення комп'ютерної безпеки, витоки конфіденційних даних, що зберігаються в комп'ютерній формі, продовжують відбуватися досить регулярно навіть у найбільших IT-

компаній, таких, як Facebook, Apple, Amazon та ін. [1]. Ці витоки торкнулися і мільйонів українських користувачів. Так, у вересні 2021 року стало відомо про те, що хакери отримали доступ до майже 53 млн. записів з персональною інформацією українців [2].

Ситуація погіршилася в період пандемії COVID -19, коли багато компаній перевели своїх співробітників на режим дистанційної роботи. У цьому режимі працівники почали масово підключатися до корпоративних мереж зі своїх особистих персональних комп'ютерних пристроїв, значну кількість яких не підготували до роботи з конфіденційними даними. Протягом двох років пандемії компанії активно вживали заходів, що дають змогу забезпечити безпеку даних при підключенні віддалених користувачів, проте підсумкові результати виявилися невтішними. Так, компанією Check Point Software Technologies на початку 2022 року були представлені результати дослідження, проведені за участю 1200 фахівців з інформаційної безпеки та інформаційних технологій у всьому світі. За їхніми результатами, 20% компаній все ще не запровадили критично важливі засоби забезпечення безпеки під час віддаленої роботи [3].

Цей приклад є дуже показовим – із завданням забезпечення безпеки під час роботи з корпоративними даними на особистих комп'ютерах користувачів не змогли повноцінно впоратися й корпоративні спеціалізовані підрозділи, основним завданням яких є захист інформації, що в такому разі очікується від звичайних користувачів.

В умовах воєнного стану в Україні ситуація ще загострилася. Тепер дані, що зберігаються на персональних комп'ютерних пристроях користувачів, можуть потрапити в руки ворога і використовуватися противником у своїх цілях. Причому їм може бути використана будь-яка інформація, виявлена на пристрої, включаючи і ту, що у мирний час не була конфіденційною чи секретною. Особливістю поточного моменту є те, що шанси отримання безпосереднього доступу до самого комп'ютерного пристрою (а не тільки віддаленого через мережу) у противника збільшилися на порядок. Особливої гостроти цієї ситуації додає можливість втрати користувачем своїх комп'ютерних пристроїв під час вимушеної евакуації, і, як наслідок – влучення цих пристроїв у чужі руки.

Виходячи з вищевикладеного, безумовно, є необхідним вживання термінових заходів щодо безпеки особистих комп'ютерних пристроїв. Крім уже відомих заходів, таких, як використання тільки легального пропрієтарного або вільно розповсюджуваного програмного забезпечення, обов'язкового використання антивірусних програм та своєчасного резервного копіювання, необхідно використовувати і додаткові. До таких, наприклад, можна віднести використання хмарних технологій та шифрування дисків комп'ютера.

Навіть безкоштовний особистий обліковий запис, отриманий у одного із західних провайдерів хмарних технологій, дає можливість розмістити у хмарному сховищі до 5 гігабайт файлів. Цього обсягу цілком вистачає для збереження великої кількості файлів текстових документів, табличних даних, документів у

форматі Word чи Excel. При платному доступі доступні сховища обсягом від одного терабайта та вище, що дозволяє зберігати у хмарі графічну та відео інформацію.

Важливість хмарних технологій повною мірою змогли оцінити люди, які змушені терміново змінити своє місце проживання або евакуюватися. Дані, збережені в хмарному сховищі, залишилися для них доступними навіть з огляду на те, що їхні особисті комп'ютери залишилися в інших містах. Крім того, дані, збережені в тільки хмарі, будуть недоступні для сторонніх осіб, які вирішили скористатися чужими комп'ютерами, що потрапили в їхні руки.

15 березня 2022 року Верховна Рада України прийняла за основу та в цілому Закон «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» за №7152.

У проекті Закону зазначається, що «власники системи для забезпечення належного функціонування систем та захисту інформації, що обробляється в них … забезпечують створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх зберігання, у тому числі за межами України … можуть розміщувати державні інформаційні ресурси та їх резервні копії на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування».

Додатково у проекті Закону зазначається, що: «Забороняється ведення публічних електронних реєстрів, за допомогою хмарних ресурсів та/або центрів обробки даних, що розміщені на території України, де органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та територіях держав, які входять до митних та воєнних союзів з такими державами» [4].

Шифрування дисків комп'ютера при використанні операційних систем сімейства MS Windows (починаючи Windows 7) може бути здійснено за допомогою входить до комплекту постачання професійної версії цієї операційної системи програми BitLocker.

Шифрування дисків за допомогою BitLocker можна проводити як на комп'ютерах із вбудованою (або додатково встановленою) апаратною підтримкою шифрування за допомогою модуля TPM (Trusted Platform Module), так і на комп'ютерах без апаратного TPM. При цьому можна шифрувати і окремі логічні диски (включаючи системні диски і диски з даними), на які може бути розбитий фізичний накопичувач комп'ютера. Крім того, за допомогою BitLocker можуть бути зашифровані і зовнішні накопичувачі, такі, як USB флеш-накопичувачі та зовнішні жорсткі диски.

Можливість шифрування дисків на комп'ютерах, де апаратний модуль TPM не встановлено, забезпечується тим, що ці сучасні процесори здатні програмно емулювати роботу апаратного модуля TPM. При цьому на багатьох старих материнських платах (розроблених ще до виходу Windows 11) необхідно включити підтримку як апаратного, так і програмного TPM в BIOS комп'ютера.

При запуску комп'ютера, системний диск якого було зашифровано за допомогою програми BitLocker, у разі використання старих материнських плат потрібно ввести пароль на сам BitLocker. У нових системах достатньо ввести пароль (або пін-код) тільки на вхід до системи Windows. У разі підключення зовнішнього накопичувача, зашифрованого за допомогою BitLocker, необхідно ввести пароль для розблокування. У тих випадках, коли користувач забув пароль до диска, зашифрованого за допомогою BitLocker, доступ до накопичувача можна отримати за допомогою ключа шифрування, який можна зберегти не тільки в письмовому вигляді, а й у хмарному сховищі (що є найбільш безпечним та зручним варіантом збереження) .

Зловмисник, який одержав фізичний доступ до комп'ютера, не зможе увійти в систему, не знаючи пароля. Якщо ж накопичувач буде вилучено з комп'ютера – прочитати дані на іншому пристрої з цього накопичувача неможливо.

На комп'ютерах, вироблених корпорацією Apple, що працюють під керуванням операційної системи macOS, аналогічні функції шифрування диска виконують програма FileVault та апаратний модуль Apple T2 Security Chip.

Як видається, шифрування за допомогою таких програм є досить надійним. Однак, як було зазначено вище, доступ до зашифрованого диска можна отримати після введення пароля (або пін-коду) Windows. А такий пароль чи пін-код можна отримати від користувача методом соціальної інженерії чи просто підібрати його. За наявності фізичного доступу зловмисника до комп'ютера такий злом навіть за наявності шифрування диска за допомогою BitLocker/FileVault стає питанням часу. З цієї причини реальний захист може забезпечити лише фізичне видалення накопичувача з комп'ютера, наприклад, перед терміновою евакуацією. Зчитати інформацію із зашифрованого накопичувача без того комп'ютера, на якому його було встановлено, буде практично неможливо.

Але з видаленням накопичувача пов'язана ще одна проблема - конструкція комп'ютера повинна дозволити користувачеві зробити швидке вилучення накопичувача без руйнування конструкції комп'ютера. Однак більшість ноутбуків і моноблоків мають конструкцію, що дозволяє розібрати комп'ютер тільки в умовах майстерні.

З урахуванням вищевикладеного, можна дати такі рекомендації: при покупці основного робочого комп'ютера слід врахувати можливість виникнення необхідності самостійного вилучення накопичувача; файли, які є конфіденційними або можуть бути такими в умовах надзвичайного або військового стану, слід, по можливості, зберігати в хмарному сховищі; диски комп'ютера повинні бути зашифрованими, а у разі використання ноутбуків або моноблоків, всі файли,

створені особисто користувачем і які не зберігаються в хмарному сховищі, необхідно зберігати на зашифрованому зовнішньому жорсткому диску. Крім того, користувач повинен мати необхідний рівень знань для роботи із програмами шифрування дисків та окремих файлів.

Список використаних джерел:

1. Nearly 26M Amazon, Facebook, Apple, eBay user logins stolen by hackers. URL: http://surl.li/bzmzi
2. Устимович Ю. Масштабная утечка данных: хакеры «слили» почти 53 млн записей с персональной информацией украинцев. URL: https://thepage.ua/news/masshtabnaya-utechka-dannyh-hakery-slili-dannye-ukraincev
3. Check Point: большинство организаций до сих пор не обеспечили защиту удаленных сотрудников. URL: https://ko.com.ua/check_point_bolshinstvo_organizacij_do_sih_por_ne_obespechili_zashhitu_udalennyh_sotrudnikov_140240
4. Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Проект Закону України №7152 від 13.03.2022. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39215

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТІ

Чеснок Б. О.

студент 1-го курсу факультету міжнародно-правових відносин Національного університету «Одеська юридична академія»

Право на захист персональних даних та недоторканність приватного життя є одним із основних прав людини. Зі швидким розвитком цифрових технологій та Інтернету це право було серйозно підірвано.

Час, коли ми живемо, так звана «ера великих даних», характеризується обробкою величезної кількості різноманітних даних. Наша особиста інформація розглядається як «нова нафта». Компанії фактично стягують плату з клієнтів за свої «безкоштовні» послуги, просячи їх залишати все більше особистих даних. Ну, всі ми знаємо стару приказку: «Безкоштовних обідів не буває». Інформація про користувачів, їхню діяльність та поведінку в мережі Інтернет використовується для: аналізу та створення особистих соціально-психологічних профілів; цільове розміщення комерційних продуктів з урахуванням індивідуальних особливостей та потреб користувачів (так званий one-to-one marketing) тощо.

Діти, будучи наймолодшими користувачами Інтернету, опинилися в центрі ринку персональних даних, що постійно зростає. Особи, які не досягли 18 років (діти) відповідно до чинного законодавства також належать до суб’єктів відносин, пов'язаних із персональними даними.

Згідно зі ст. 4 Закону України «Про захист персональних даних» суб'єктами відносин, пов'язаних із персональними даними, є суб'єкт персональних даних;

володілець персональних даних; розпорядник персональних даних; третя особа; Уповноважений Верховної Ради України з прав людини.

Персональними даними є всі дані, що стосуються особи, на підставі яких ця особа може бути ідентифікована (прямо чи опосередковано) і, таким чином, її конфіденційність може бути поставлена під загрозу [1].

До персональних даних належать:

- Ім'я та прізвище.
- Адреса проживання.
- Адреса електронної пошти.
- Світлина.
- IP – адреса.
- Місцезнаходження людини.
- Інформація, що використовується для аналізу та створення профілів користувачів (робочі здібності, економічний статус, особисті інтереси, поведінка, споживчі звички, мобільність тощо).
- Онлайн-поведінка людини (дані збираються за допомогою файлів cookie).

Європейський загальний регламент захисту даних (GDPR), який набув чинності з 25 травня 2018 року в країнах Європейського Союзу, стосується особистої інформації та є новим стандартом захисту особистих даних та конфіденційності громадян. У цьому Регламенті велика увага приділяється захисту конкретних категорій особистої інформації:

- Расова або етнічна приналежність.
- Релігійна приналежність.
- Членство у профспілках.
- Сексуальна орієнтація.
- Інформація про здоров'я (персональні дані щодо фізичного та психічного здоров'я людини, включаючи надання медичних послуг).
- Біометричні дані.
- Генетичні дані (персональні дані, що стосуються успадкованих або набутих генетичних характеристик людини, що надають унікальну інформацію про фізіологію або здоров'я людини та отримані шляхом аналізу біологічного зразка людини).

Право на недоторканність приватного життя та захист персональних даних є одним із основних прав, передбачених Конвенцією Організації Об'єднаних Націй про права дитини (стаття 16). Це право однаково відноситься і до цифрового середовища.

За словами Хелен Ніссенбаум, професора інформаційних технологій Корнельського університету, недоторканність приватного життя – це не право на секретність чи контроль, а право на належний потік особистої інформації. Що це означає? Це означає, що залежно від ситуації та контексту людина може оцінити та вирішити, чим поділитися з іншими у цифровому середовищі. Іншими

словами, людина має право знати, як і для яких цілей використовуються її дані, хто і як довго їх зберігає, а також, кому доступна така інформація. Особа також може запитати про видалення особистих даних або виправлення невірних [2].

Коли йдеться про дітей, постає питання, чи здатні вони зрозуміти, якою особистою інформацією не слід ділитися з іншими, у яких ситуаціях і чому? Хоча вони дуже стурбовані тим, яка особиста інформація потрапить до рук їхніх батьків або друзів, діти не розуміють, чому великі корпорації (такі як Facebook, Instagram або Snapchat) цікавляться такою інформацією. Згідно з деякими дослідженнями, діти дбають про своє приватне життя у відносинах з оточуючими, але, незважаючи на це, діляться нею публічно; тобто вони не знають про неправомірне використання персональних даних у комерційних цілях та в інституційному контексті (наприклад, у школі, медичному закладі).

У зв'язку з тим, що вони недостатньо обізнані про ризики, наслідки, захист і права, пов'язані з обробкою персональних даних, діти заслуговують на особливий захист конфіденційності в Інтернеті (GDPR).

Персональні дані в Інтернеті можна розділити на три категорії:

1. Активні цифрові сліди – інформація (про себе або інші), яку користувачі залишають при використанні Інтернету, як правило, свідомо, хоча і не обов'язково навмисно (наприклад, при купівлі деяких товарів, завантаженні контенту з Інтернету, завантаженні фотографій, створенні профілів у соціальних мережах).

2. Пасивні цифрові сліди – інформація, яку користувачі залишають в Інтернеті під час його використання, переважно неусвідомлено (наприклад, через файли cookie, відбитки пальців, дані про місцезнаходження, використання розумних речей та розумних іграшок).

3. Інформація, отримана шляхом аналізу перших двох категорій даних з використанням алгоритмів (через процес профілювання), можливо у поєднанні з іншими джерелами даних.

Велика кількість вебсайтів та програм (наприклад, відеоігри, соціальні мережі, сайти знайомств або азартні ігри) вимагають, щоб користувачі вказували свій вік під час створення профілів (реєстрації). Ці послуги мають мінімальний віковий ліміт для їх використання.

Причини, з яких більшість таких сервісів вимагають мінімального вікового обмеження для їх використання, полягають у наступному:

1. Деякі вебсайти та програми за змістом, призначенням або через те, що вони збирають і зберігають дані про користувачів, призначені для дорослих (людей старшого віку), а не для дітей.

2. Відповідно до Закону США про захист конфіденційності дітей в Інтернеті (COPPA) жодна організація або особа, яка користується послугами в Інтернеті (включаючи власників вебсайтів соціальних мереж), не може збирати особисті дані осіб віком до 13 років без дозволу їхніх батьків або опікунів. . Більшість постачальників послуг встановили вікове обмеження на використання своїх

послуг, щоб уникнути отримання батьківської згоди для осіб, молодших за встановлений вік. Це обмеження чітко зазначено в Умовах та положеннях, вимагаючи від користувачів дотримання цих умов, перш ніж вони почнуть користуватися послугами. Щоб захистити користувачів, а також самих себе (щоб уникнути порушення закону), вебсайти зобов'язуються видаляти будь-який профіль, створений особою віком до 13 років [3].

В умовах обслуговування популярної соціальної мережі Facebook сказано, що сайт не можуть використовувати особи, які не досягли 13-річного віку (або особи, які не досягли «мінімального віку, встановленого законом у вашій країні для використання наших продуктів»). Хоча більшість соціальних мереж (таких як Facebook, Snapchat, Twitter, Instagram, Skype) вимагають мінімального вікового обмеження в 13 років (є також деякі інтерактивні сервіси, розроблені спеціально для дітей молодшого віку), дослідження показують, що великий відсоток дітей (як у Сербії , так і в інших місцях) починають використовувати ці мережі в більш ранньому віці, ніж запропоновано.

Багато батьків стикаються з проблемою дозволити своїм дітям створити профіль у соціальній мережі у більш ранньому віці, ніж належить. Можливо мати особистий профіль у віці молодше встановленого лише у тому випадку, якщо користувач вводить неправильний вік під час створення профілю.

Для того, щоб захистити свої персональні дані в Інтернеті слід пам'ятати про те, що Інтернет є загальнодоступним простором і дані, розміщені в Інтернеті, доступні для громадськості, пам'ятати про те, що конфіденційність в онлайн-середовищі така ж важлива, як і в реальному світі, про те, що ви залишаєте свої особисті дані на будь-якій вебсторінці, яку ви відвідуєте і тим самим формуєте свою унікальну цифрову особистість - що дозволяє однозначно ідентифікувати вашу особу в мережі.

Список використаних джерел:

1. Про захист персональних даних: Закон України від 01.06.2010 р. №2297-VI *Відомості Верховної Ради України*. 2010. №34, стор. 1188, стаття 481.
2. Dobrinka Kuzmanović, PhD: Personal data protection and privacy on the Internet URL: https://cutt.ly/zHz6vOQ.
3. Захист персональних даних. URL: https://cutt.ly/MHz5ZJw

Науковий керівник: доцент Чанишев Р. І.

Секція 3. УПРАВЛІНСЬКІ ТА ЕКОНОМІЧНІ АСПЕКТИ РОЗВИТКУ СУЧАСНОЇ ІТ ІНДУСТРІЇ

ПЕРЕФОРМАТУВАННЯ ІТ СЕКТОРУ УКРАЇНИ В УМОВАХ ВІЙНИ

Горбаченко С. А.

доктор економічних наук, професор, завідувач кафедри кібербезпеки Національного університету «Одеська юридична академія»

Протягом останніх років ІТ індустрія була локомотивом розвитку вітчизняної економіки майже за всіма показниками: від експортних надходжень до середньої заробітної плати в галузі. І навіть в умовах війни більшість ІТ компаній зберегли не тільки потенціал, а й поточних клієнтів і контракти попри такі ризики, як: невиконання проєктів через війну, мобілізацію ключових інженерів, нестабільність в країні, фізичну безпеку даних, кіберзагрози, відсутність інтернету, неможливість працювати з розробниками, які знаходяться на території активних військових дій.

У кількісному виразі за даними І кварталу 2022 р. вітчизняна ІТ індустрія забезпечила в умовах війни рекордних 2 млрд дол. США експортних надходжень. Адже аналогічний показник у 2021 році становив 1,44 млрд дол. США. Таким чином, обсяг ІТ-експорту збільшився на 28%. У галузі працюють близько 300 тис. спеціалістів і 70% з них з початку 2022 р. змінили місце проживання. Крім того у березні 2022 р. українська ІТ-галузь зберегла 96 % обсягу експорту ІТ послуг (522 млн. дол. США) в порівнянні з аналогічним періодом минулого року (546 млн. дол. США) чим довела свій запас міцності в умовах нестабільності та підвищених ризиків [1].

Паралельно із цим український ІТ бізнес припинив співпрацю з РФ, адже, зокрема, з 10 найбільших вітчизняних ІТ компаній 3 мали там офіси (EPAM, Luxoft, DataArt). І хоч і не одразу після початку війни, але всі вони заявили, що згортають бізнес у країні-агресорі.

Основні економічні побоювання щодо функціонування ІТ сектору у військових умовах зводилися, в першу чергу, до двох пунктів: втрата клієнтів, проєктів, а отже робочих місць і масова релокація фахівців за кордон. Дійсно, в перший місяць, внаслідок активних бойових дій роботу втратили близько 5-7% фахівців галузі. У подальшому ж звільнення обумовлювалися, насамперед, процесами оптимізації бізнесу внаслідок скорочення діяльності. До цього були вимушені вдатися насамперед великі компанії, такі як Rozetka, EVO, Нова Пошта та багато інших.

Якщо говорити про внутрішні територіальні зміни та географію звільнень, менше за всіх постраждали підприємства та фахівці Львова, Тернополя та Івано-Франківська. У Києві та Одесі дуже складним був перший місяць війни, проте

потім ситуація дещо вирівнялася. Найбільше ж постраждало ІТ середовище Дніпра, Харкова та Запоріжжя.

Український уряд декларує допомогу ІТ-сектору для підтримки його функціонування під час війни, зокрема у питанні щодо тимчасового звільнення від мобілізації ІТ фахівців, які мають особливу цінність для підприємств. Отже за оцінками фахівців в ІТ середовищі частка мобілізованих не перевищує 5%, плюс ще деякий відсоток складають ті хто служить добровільно.

Особливості ІТ сектору дозволяють перенести в інші країни не тільки розробку програмних продуктів, а й підтримку клієнтів, більшість ІТ послуг і ряд допоміжних бізнес-процесів. Тому в контексті релокаційних аспектів увага роботодавців була сфокусована в першу чергу на безпеці працівників та їхньому оперативному переміщенні зі сходу країни в безпечні місця – на захід або за кордон. Звісно, значна частин ІТ фахівців покинула Україну, причому вказаний процес активізувався від самого початку 2022 р. Серед країн куди виїжджали ІТ фахівці лідирують Польща (35%) та Німеччина (10%). Так само працюють команди в Ірландії, Болгарії, Португалії. Слід зауважити, що понад 90% ІТ фахівців допомагають фінансово армії, благодійним фондам або ж сам є волонтерами.

У контексті внутрішньої релокації найбільше ІТ фахівців переїхало до Львівської області (11%), Івано-Франківської області (6%) та Закарпаття (9%). У переважній більшості ІТ фахівців внаслідок релокаціїї не змінилися а ні навантаження, а ні доходи. Середня пропонована заробітна плата у всіх актуальних вакансіях на квітень 2022 р. складає 86,5 тис. грн. Найбільше пропозицій роботи зі щомісячною компенсацією від 44,2 тис. грн (36%). Ще у чверті вакансій зарплата складає від 77,5 тис. грн. [2].

Як свідчить практика найлегше знайти нове місце роботи проєктним менеджерам, розробникам та фахівцям DevOps/SRE, QA, Data Scientists та HR. Найскладніше працевлаштуватися sales менеджерам, системним адміністраторам, фахівцям технічної підтримки, дизайнерам та маркетологам. Проте, незважаючи на складнощі, частка ІТ фахівців, які все ще знаходяться в пошуках роботи не перевищує 5%.

Таким чином в нових умовах ІТ галузь залишається фінансово стабільною, забезпечує регулярні валютні надходження в економіку України та державний бюджет. Для подальшого розвитку вітчизняного ІТ сектору в умовах війни потрібно зробити такі додаткові кроки.

1. Створення умов для масового навчання та перенавчання на ІТ спеціальності (певні кроки в цьому напрямі вже зроблено адже такі компанії як Genesis, EPAM, Beetroot вже або розробили нові курси для полегшеного входу у професію або зробили власні курси безкоштовними).

2. Формування пропозиції для великих іноземних компаній (із застосуванням підтримки на державному рівні) щодо залучення вітчизняних фахівців на умовах аутсорсінгу, можливо, навіть, у формі державного аутстаффінгового агентства.

3. Перехід от великих офісів до мобільних команд для яких легше здійснити оперативну релокацію.

Список використаних джерел:

1. Українська IT-Індустрія: перезавантаження в умовах війни. URL: https://itukraine.org.ua/ukrainian-it-industry-reboot-in-wartime.html
2. Як війна вплинула на IT-сферу: зарплати, вакансії, локації. URL: https://minfin.com.ua/ua/2022/04/06/83259219/

АУТСОРСИНГ В УКРАЇНІ Й У СВІТІ: ОСОБЛИВОСТІ, ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ

Дем'янова Т.І.

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Аутсорсинг – поняття, яке міцно ввійшло в наш побут, означає комплекс заходів, спрямованих на передачу підприємством певних процесів і функцій іншої організації, яка професійно спеціалізується у сфері поставлених завдань. Також аутсорсинг має більш тривалий характер взаємодії порівняно з разовими послугами, які запитуються більш ситуативно. Найчастіше аутсорсингові послуги надають в IT-сфері, але крім цього популярні у сферах логістики, ресурсного забезпечення виробничих процесів, маркетингових послуг, рекрутингу, бухгалтерського обліку, обробки й систематизації інформації, медичних послуг, адміністрування

Види аутсорсингу:

- Офшоринг – замовник і виконавець перебувають на території різних країн, при цьому виконавець є підрозділом замовника.
- Аутсорсинг – замовник і виконавець перебувають на території однієї країни, при цьому виконавець є незалежним підприємством.
- Офшорний аутсорсинг – є змішаним видом. Замовник і виконавець перебувають на території різних країн, але при цьому виконавець є незалежним підприємством.
- Виробничий аутсорсинг – передача виробничих функцій виконавцеві.
- Аутсорсинг бізнес-процесів – передача виконавцеві процесів, що не є основним видом діяльності замовника.
- IT-аутсорсинг – передача на обслуговування інформаційних систем замовника.

IT-аутсорсинг в економіці України

IT-аутсорсинг є частковою або повною передачею робіт з підтримки, обслуговування та модернізації IT-інфраструктури до компаній, що спеціалізуються

на абонентському обслуговуванні організацій і мають штат фахівців різної кваліфікації.

Серед найпоширеніших на даний час видів ІТ-аутсорсингу слід виділити такі:

- виведення в іншу країну другорядних служб підтримки інфраструктури виведення в іншу країну некритичних для бізнесу процесів, що потребують значного обсягу некваліфікованої праці
- розробка програмного забезпечення на замовлення.

Уже сьогодні розвиток ІТ-аутсорсингу в Україні дозволяє досягти позитивних макроекономічних ефектів, що впливають на економічний розвиток країни. У перспективі ці ефекти здатні обумовити структурні перетворення, які формуватимуть нові тенденції української економіки.

До ефектів розвитку ІТ-аутсорсингу в нашій державі можна віднести:

- покращення структури ринку праці;
- приплив іноземної валюти та поліпшення платіжного балансу країни;
- збільшення внутрішнього попиту на споживчому ринку;
- подолання розшарування населення й формування середнього класу;
- зміцнення фінансової безпеки держави.

90 % ІТ послуг України надає на принципах аутсорсингу іншим країнам, а за темпами зростання цього сегмента ІТ в світі ми поступаємося тільки Індії.

У 2003 р. обсяг ринку ІТ-аутсорсингу в Україні становив 110 млн дол., у 2007 р. – 544 млн дол., у 2011 – 1,1 млрд дол., а у 2014 р. цей показник сягнув майже 2,4 млрд дол.

Світовий аутсорсинг

Використання людського ресурсу – це основа успішної роботи аутсорсингу у світі. Серед країн-виконавців лідирують Індія, Китай, до яких надходять замовлення з країн Європи, США, Японії. На аутсорсингу замовників з європейських країн частіше працюють виконавці в країнах Східної та Центральної Європи, Китаї, Індії. Відносно високих показників динаміки ринку вдалося досягти за рахунок розвитку офшорного аутсорсингу в країнах по сусідству з меншими ресурсними витратами. Своєю чергою, Україна, як країна, орієнтована на експорт своїх послуг, постачає свої послуги переважно до США, країн Євросоюзу та Ізраїлю. На аутсорсингу замовників з європейських країн частіше працюють виконавці в країнах Східної та Центральної Європи, Китаї, Індії. Відносно високих показників динаміки ринку вдалося досягти за рахунок розвитку офшорного аутсорсингу в країнах по сусідству з меншими ресурсними витратами. Своєю чергою, Україна, як країна, орієнтована на експорт своїх послуг, постачає свої послуги переважно до США, країн Євросоюзу та Ізраїлю.

Тенденції та перспективи

З розвитком технологій одним із сучасних видів аутсорсингу можна назвати краудсорсинг (англ. crowdsourcing: crowd – юрба і sourcing – використання ресурсів), коли до вирішення поставлених завдань може залучатися широке коло осіб за допомогою інформаційно-комунікаційних технологій в усьому світі.

Зростання звертання до краудсорсингу спричинить перегляд усталених договірних соціально-трудових відносин у світі.

Співробітники, що залучаються в межах краудсорсингу, не підкоряються вказівкам і розпорядженням замовника й вільні самостійно обирати місце та час, що виділяються для роботи. Співпраця відбувається в простій і незобов'язуючій формі. Часто на краудсорсингових платформах прямо вказується, що краудсорсинг не тягне за собою встановлення постійного працевлаштування.

Висновки: світ змінюється набагато швидше з настанням четвертої промислової революції (індустрії 4.0), ринок праці піддається незаперечному впливу, коли більшість робіт спрощується за допомогою технологій; одним з наслідків стає відступлення від звичних урегульованих трудових відносин і структур. Наше робоче оточення і середовище, до яких ми звикли, радикально змінюються вже сьогодні.

Список використаних джерел:

1. О. Стахурська, партнер, Taylor Wessing Ukraine. Аутсорсинг в Україні й у світі: особливості, тенденції та перспективи. URL: https://uz.ligazakon.ua/ua/magazine_article/EA010850
2. Аутсорсинг_в_Україні. URL: https://uk.wikipedia.org/

Науковій керівник: професор Горбаченко С.А.

ІНСТРУМЕНТИ ПРОЄКТНОГО МЕНЕДЖМЕНТУ В ІТ

Дяченко А.О.

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету "Одеська юридична академія"

В IT, project management (PM) – це дисципліна, що поєднує процедури, принципи та політику ведення бізнесу. Вона керує проектом від розробки концепції до завершення проекту.

Загальний (функціональний) та проектний менеджмент відрізняється тим, що:

- функціональний стабільний. Мета: підтримати та примножити. Є відпрацьований шаблон, він працює постійно.
- проектний мінливий. Ціль: результат за будь-яку ціну. Є deadline.

Причиною переходу від загального менеджменту до PM найчастіше стає надійність – замість відносної абстрактної перспективи до передбачуваних результатів.

Міжнародна Асоціація Управління Проектами (IPMA) провела дослідження, за результатами якого новий підхід заощадить вам близько 20-30% часу та 15-20% ресурсів.

В Америці послуги для ведення бізнесу існують з 1987 року, у нас же заповітна 1С з'явилася лише в 1991 році. Розвиток технологій від автоматизованого бухгалтерського обліку та CRM для call-центрів до повноцінного віртуального середовища централізованого контролю та взаємодії в компанії було тривалим, але плідним.

На 2017 рік інструменти управління проектами стали найпоширенішим явищем. Розвинувся дуже різноманітний ринок сервісів, що відрізняються галузевим софтом, функціями та наявністю інтеграції з іншими програмами. Тепер вони можуть бути з розширеннями та мобільними версіями.

Для спілкування з співпрацівниками використовують такі інструменти:

Gmail. З плюсів: дуже зручний інтерфейс, і за своїми можливостями він значно випереджає конкурентів (той самий MS Outlook); можна впорядковувати та групувати листи за папками; безпека в Google завжди була і залишається на висоті; зручний додаток для Android та iOS. З мінусів: обмеження обсягу пам'яті для зберігання листів — 15 Гб, які доводиться ділити з Google-диском.

Тут не обійтися без *Slack*, який вже практично став стандартом корпоративного використання. У ньому легко та зручно створювати групи, канали, здійснювати дзвінки без використання сторонніх сервісів, нагадувати учасникам про meetings та створювати опитування.

Останнім часом для швидкого обміну інформацією в рамках однієї групи розробників та IT-команди загалом усе активніше використовується *Telegram*.

Для відеозв'язку використовують Zoom та Webex.

Інструмент для постановки та моніторингу завдань: *Jira*.

По-перше Jira це баг-трекер, тобто система для контролю помилок у програмному коді. Але більшість компаній використовують її як інструмент управління проектами.

Плюси. Є інтеграція з іншими інструментами і просунуті фільтри. Цей проект люблять розробники за можливість будь-якої миті побачити процеси проекту в необхідному масштабі. Можливості можна розширити плагінами.

Мінуси. Багато функцій доступні лише через інтеграцію з іншими сервісами. І підходить Jira лише для команд, які використовують методології Scrum та Kanban.

Інструменти для роботи з проектною документацією.

Проєктним менеджерам часто необхідно доповнювати документацію схемами, діаграмами та мокапами. Тоді в хід ідуть такі сервіси, як Lucidchart, Gliffy, Draw.io.

Про *Draw.io*:

Плюси. гарний набір інструментів та функцій для створення організаційних діаграм, блок-схем (флоучартів), мережевих діаграм, UML; широкий вибір форматів для завантаження файлів; можливість інтеграції з іншими застосунками; інструмент повністю безкоштовний та працює на будь-якому пристрої.

Отже, будь-яким проектом можна керувати за допомогою зв'язування спеціалізованого софту. Календарі, таск-менеджери, рішення для зберігання коду, графіки, текстів, хмарні послуги для спільної роботи над завданням - рішень дійсно багато, причому якісних.

Але все це лише допоміжний інструмент. Для того щоб бути справжнім менеджером проектів і не завалити перше ж своє завдання, потрібна довга практика.

Список використаних джерел:

1. 10 инструментов для управления проектами: эффективность, постановка задач и общение. URL: https://skillbox.ru/media/management/10_instrumentov_dlya_pm/
2. Інструменти професії: з чим працює проєктний менеджер в IT. URL:https://happymonday.ua/z-chym-pratsyuye-project-menedzher

Науковий керівник: професор Горбаченко С.А.

РИЗИКОВІСТЬ ТА БЕЗПЕКА ІНВЕСТОРІВ У ВИКОРИСТАННІ ІНТЕРНЕТ-ТЕХНОЛОГІЙ

Захарченко Н.В.

доктор економічних наук,
професор кафедри економіки, права та управління бізнесом
Одеського національного економічного університету

У зв'язку зі збільшенням кількості сайтів у мережі Інтернет, що пропонують українським інвесторам можливість торгівлі акціями американських та інших іноземних елементів з використанням мережі Інтернет, зростає рівень махінацій та різних шахрайських схем. Діяльність на ринку цінних паперів в мережі Інтернет має високий ступінь ризику. По-перше, це пов’язано з природою самої діяльності, а по-друге, через ризик залученості до шахрайських схем та ринкових маніпуляцій.

Проаналізуємо існуючі види таких схем за результатами аналізу роботи Комісії з цінних паперів і бірж США.

1. Схема «збільшити і скинути» – вид ринкової маніпуляції, що полягає у одержанні прибутку з допомогою продажу цінних паперів, попит на який був штучно сформований. Маніпулятор, називаючись обізнаною особою і поширюючи неправдиву інформацію про емітент, створює підвищений попит на певні цінні папери, сприяє підвищенню їхньої ціни, потім здійснює продаж цінних паперів за завищеними цінами. Після маніпуляцій ціна на ринку повертається до свого вихідного рівня, а інвестори опиняються у збитку. Цей прийом використовується в умовах нестачі або відсутності інформації про компанію, цінні папери якої рідко торгуються.

2. Схема фінансової піраміди під час інвестування коштів, використовуючи Інтернет-технології, повністю повторює класичну фінансову піраміду. З використанням цього прийому інвестор отримує прибуток виключно з допомогою залучення у гру нових инвесторів [2].

Схема «надійного» вкладення капіталу – поширення через Інтернет інвестиційних пропозицій із низьким рівнем ризику та високим рівнем прибутку. Це пропозиції неіснуючих, але дуже популярних проектів, таких як вкладення у високоліквідні цінні папери банків, телекомунікаційних компаній, з безумовними гарантіями повернення вкладеного капіталу та високими прибутками.

3. «Екзотичні» пропозиції – наприклад, поширення через Інтернет пропозиції акцій костариканської кокосової плантації, що має контракт з мережею американських універмагів із банківською гарантією отримання основної суми інвестицій плюс 15% прибутку.

4. Шахрайства з допомогою банків – у тому, що шахраї, прикриваючись іменами і гарантіями відомих фінансових установ, пропонують інвесторам вкладення грошей у нічим не забезпечені зобов'язання з нереальними розмірами доходності.

5. Нав'язування інформації – часто інвесторів вводять в оману недостовірної інформації про емітент, перебільшеними перспективами зростання підприємств, цінних паперів яких пропонуються. Інформація може бути поширена серед широкого кола користувачів мережі найрізноманітнішими способами: розміщена на інформаційних сайтах, електронних дошках оголошень, інвестиційних форумах, розіслана електронною поштою [1].

Анонімність, яку надає Інтернет, можливість охоплення великої аудиторії, висока швидкість і набагато нижча вартість розповсюдження інформації, робить Інтернет найбільш зручним інструментом для шахрайських дій.

Таким чином, щоб уникнути втрат коштів при інвестуванні на іноземних фондових ринках, інвестору слід дотримуватися наступних правил:

1) усвідомлено підходити вибору об'єкта інвестицій;

2) звертатися до послуг брокера;

3) ретельно обмірковувати різноманітні “привабливі” пропозиції;

4) виявляти обережність при наданні інформації про паролі доступу до інвестиційного рахунку;

5) використовувати лімітні накази для запобігання купівлі або продажу акцій за цінами вищими або нижчими за бажану. Лімітний наказ передбачає наявність наперед визначеної інвестором ціни виконання.

Крім означених шахрайських схем та ринкових маніпуляцій підвищення рівня ризику для інвесторів зросло посиленням російської військової агресії. Тому для прийняття інвестиційного рішення слід провести детальний аналіз інформації про об’єкт інвестування, оцінити всі ймовірні та можливі ризики, не вдаватись до високих обіцяних відсотків по прибутку, убезпечити можливі ризики та наслідки.

Список використаних джерел:

1. Захарченко Н.В., Вольневич Ю.С. Сучасні технології в бізнес-аналітиці. *Економічна аналітика: сучасні реалії та прогностичні можливості:* зб. матеріалів Міжн. наук.-практ. конф. (19 квітня 2019 р.). Київ: КНЕУ, 2019. С. 113-115.
2. Інформаційні технології в бізнесі. Частина 1: Навч. посіб. / [Шевчук І.Б., Старух А.І., Васьків О.М. та ін.]; за заг. ред. І.Б. Шевчук. Львів: Видавництво ННВК «АТБ», 2020. 455 с.
3. Приходько В.П. Інвестиційна безпека як важливий чинник подолання фінансово-економічної кризи. URL: http://www.investplan.com.ua/pdf/16_2013/3.pdf

РОЛЬ ТАРГЕТОВАНОЇ РЕКЛАМИ В БІЗНЕСІ

Нігуренко А. С.

студентка 1-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У зв'язку з військовим положенням в Україні та складною економічною ситуацією у світі, бізнесу, як ніколи, потрібні клієнти, щоб продовжувати своє існування. Оскільки люди все більше часу починають проводити вільний час в Інтернеті, в першу чергу, в соціальних мережах, то таргетована реклама, якнайкраще може допомогти підприємству будь-якої сфери.

Таргетинг (з англ. Targening, націлювання) – це маркетинговий інструмент, який показує рекламне оголошення цільової аудиторії в Інтернеті. Мета таргетингу – відсіяти нецільову аудиторію та зосередитися на потенційних клієнтах. Система передбачає пошук цільової аудиторії за певними параметрами, які задаються в налаштуваннях таргету.

З огляду на вищевказане, можна сформулювати основні завдання таргетованої реклами:

1. Збільшити ефективність продажів.
2. Здійснити візуальне знайомство аудиторії з атрибутами компанії (логотип/назва/банер запам'ятовується цільовій аудиторії, навіть якщо в даний момент послуга або пропозиція не актуальні, а значить, при необхідності подальшої замовлення товару або послуги, є великий шанс, що компанія буде фігурувати у списку агентів по угоді).
3. Оптимізувати кошти, витрачені на рекламу та просування продукту.
4. Отримати нових лідів, збільшити кількість відвідувачів на сайті, покращити конверсію.
5. Збільшити кількість відвідувачів у соцмережах.
6. Підвищити пізнаваність бренду.
7. Залучити людей з онлайн в офлайн.
8. Збільшити обсяг продажів товарів та послуг на сайті.

Таргетована реклама проводиться в соціальних мережах і на інших Інтернет-ресурсах і передбачає поступе проходження декількох етапів.

Першим етапом початку роботи таргетингової реклами є моніторинг з метою виявлення зацікавленої аудиторії з числа потенційних клієнтів. Аналіз цих даних приводить до сегментації: з більшої кількості користувачів виокремлюються цільові групи зі смаками, уподобаннями й інтересами, які максимально точно відповідають цілям і сутності рекламної кампанії. Таргетологи відбирають тільки ті цільові групи, в яких представлена найбільша кількість потенційно зацікавлених клієнтів.

Наступний етап є найбільш важливим, адже на ньому необхідно створити сам рекламний матеріал, який повинен привернути увагу цільової аудиторії і зацікавити умовою придбання. Написання рекламного повідомлення для потенційних клієнтів є найбільш важливим. На цьому ж етапі обирають й конкретні види таргетованої реклами, такі як: контекстна, тематична, геотаргетинг, тимчасова, соціальна, поведінкова.

З точки зору економчної сери таргетована реклама підходить далеко не всім. Для деяких підприємств такий варіант розвитку буде максимально вигідним. Зокрема для B2C таргетована реклама підходить ідеально, особливо для: Інтернет-магазинів; ресторанів, кафе, нічних клубів та інших подібних закладів; фітнес-центрів та спортзалів; семінарів, лекцій, курсів. Також таргетинг підходить: невеликим компаніям, які здійснюють свої послуги або продають товари для певного міста чи району; для тих, у кого є сайт з організацією переходів безпосередньо на ресурс продажу; продавцям інформаційних ресурсів, мобільних ігор і застосунків; при відсутності інших можливостей для просування, коли інші ресурси вже вичерпані і не дають очікуваних результатів; для сегменту бізнесу зі специфічним напрямком роботи.

Для інших підприємств, зокрема тих, хто працює у сфері B2B, для вузькоспеціалізованих товарів та медичних закладів таргетована реклама призведе до витрат і втраченого часу.

Отже, таргетинг дозволяє раціонально використовувати маркетинговий бюджет і отримувати максимальну вигоду від реклами. Персоналізована реклама можлива всюди: від пошукових систем до банерів. Така реклама вирішує одразу декілька завдань бізнесу. За допомогою неї про компанію дізнається більше людей і, як наслідок, більше потенційних клієнтів.

В подальшому таргетинг також має допомогти вітчизняному бізнесу збирати якісних лідів, залучати клієнтів, збільшувати продажі, дослідити клієнтів, сегментувати користувачів, інформувати про подію чи акцію, перевіряти гіпотези, працювати на імідж.

Список використаних джерел:

1. Таргетована реклама: що це, для чого вона потрібна, як ефективно використовувати? URL: https://bestmarketing.com.ua/ua/tarhetovana-reklama-shcho-tse-i-dlya-choho-vona-potribna/
2. Таргетована реклама — що це таке? Види таргетингової реклами. URL: http://delukr.kiev.ua/targetovana-reklama-shho-tse-take-vidi-targetingovoyi-reklami/
3. Что такое таргетинг и чем он полезен бизнесу. URL: https://www.carrotquest.io/blog/chto-takoe-targeting-i-chem-on-polezen-biznesu/

Науковий керівник: процесор Горбаченко С. А.

ЗМІСТ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

20 травня 2022 року
м. Одеса

Відповідальній редактор: Н. І. Логінова

Дизайнер: Р. Р. Дробожур

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ

МАТЕРІАЛИ VII ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: «ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»

20 травня 2022 року, м. Одеса