Міністерство освіти і науки України

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ

# МАТЕРІАЛИ
# 84-ої МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ ХНАДУ

Харків 2022

**ЗМІСТ**

# ОБГРУНТУВАННЯ УПРАВЛІНСЬКИХ РІШЕНЬ ПРИ РОЗРОБЦІ ТА ВПРОВАДЖЕННІ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЙ

**Фастовець В.,** магістриня гр. АМСЗІзм-21-1, доц. Добринін І.С.
ХНУРЕ

Розвиток комп'ютерних технологій і їх використання в багатьох сферах економіки є на сьогодні одним з головних факторів її ефективності. Проте прогрес в інформаційно-технічній сфері створив і потенційні загрози у вигляді розроблення нових та удосконалення вже відомих методів наукового шпигунства, котрі дозволяють швидко знаходити в комп'ютері необхідні відомості.

Крім того, у зв'язку з бурхливим розвитком локальних і глобальних обчислювальних мереж удосконалюються і методи розвідки (комерційного шпигунства), спрямовані на перехоплення інформації, що обробляється, передається, зберігається у локальних мережах. Відповідно, швидко удосконалюються і методи протидії розвідці.

Необхідно зазначити, що увійти у локальну мережу будь-якої організації можна лише при некваліфікованому налагодженні всіх елементів локальної мережі (кожного окремого комп'ютера) адміністратором системи. Не випадково останнім часом бурхливо розвиваються методи перехоплення інформації за допомогою каналів побічного електромагнітного випромінення і наведень (ПЕМВН) елементів комп'ютерних мереж.

Забезпечення інформаційної безпеки в корпоративних, міжкорпоративних, локальних обчислювальних та інших автоматизованих системах зараз набуває особливої актуальності. За даними статистики, основним джерелом загрози безпеці корпоративної мережі, як і раніше, залишаються саме легальні користувачі. Відтік або втрата конфіденційної інформації та вихід з ладу обладнання може статися внаслідок: незумисних помилок користувача; умисних шкідливих дій користувача; таємного введення в систему програм-закладок з вірусами «троянський кінь», «черв'як» тощо.

Значна кількість важливої інформації зберігається не лише на серверах, а й на робочих станціях (комп'ютерах) користувача. Ці дані можуть бути легко втрачені або розголошені, якщо не вживати відповідних заходів. За допомогою списків управління доступом (ACL) можна обмежити доступ до комп'ютера як для окремого, так і для групи користувачів. Наприклад, один з користувачів зможе читати зміст файлу, інший – вносити до нього зміни, а всі інші взагалі позбавлені доступу до файлу. Це необхідно, коли на одному комп'ютері працює кілька користувачів або в мережі підприємства не встановлено обмежень на їх реєстрацію і будь-який користувач, який має фізичний доступ до комп'ютера, може зареєструватися на ньому.

Найбезпечнішою з усіх можливих загроз при підключені до глобальної мережі Internet є злам мережі з хуліганських мотивів. В разі під'єднання комп'ютерних мереж державних установ, підприємств, науково-дослідних інститутів та організацій до глобальної мережі Інтернет слід очікувати, окрім хуліганських зламів мережі і кваліфікованого проникнення до ресурсів корпоративної мережі. Протидіяти цьому дуже складно. Тому мережу Інтернет необхідно ізолювати від внутрішніх важливих ресурсів, де зосереджені конфіденційні дані, дані для обмеженого користування і доступу. В мережах, у яких не використовується інформація з обмеженим доступом, для ізоляції, як правило, досить використати фільтруючий маршрутизатор, що виконує роль брандмауера, тобто шлюзу, який обмежує доступ до інформаційних ресурсів внутрішньої мережі підприємства.

Достатній захист від проникнення з глобальної мережі можна забезпечити за допомогою міжмережевих екранів. Проте найповніша безпека гарантується лише фізичною ізоляцією локальної мережі від мережі Інтернет.

Мета роботи: розглянути метод аналізу ієрархій, який використовується при обґрунтуванні управлінських рішень при розробці та впровадженні систем менеджменту інформаційної безпеки та навести приклад.

Метод аналізу ієрархій (MAI) — це структурований метод організації та аналізу складних рішень, заснований на математиці та психології. Він був розроблений в 1970-х роках Томасом Л. Сааті, і з

тих пір він широко вивчався та вдосконалювався. Він представляє точний підхід для кількісної оцінки ваги критеріїв прийняття рішень. Для оцінки відносної величини факторів за допомогою парних порівнянь використовується досвід окремих експертів.

Опишемо коротко метод. Нехай:

A1 ... An – множина з n елементів;

W1…Wn – співвідносяться наступним чином:

Таблиця 1 – Розрахунок відносної сили критеріїв

| | $A_1$ | … | $A_n$ |
|---|---|---|---|
| $A_1$ | 1 | … | $W_1/W_n$ |
| … | … | 1 | $A_n$ |
| $A_n$ | $W_n/W_1$ | … | 1 |

Оцінка заповненої матриці порівнянь проводиться у разі формулам (табл. 2) для обчислення вектора пріоритетів.

Таблиця 2 – Оцінка пріоритетів

| | $A_1$ | … | | $A_n$ | | |
|---|---|---|---|---|---|---|
| $A_1$ | 1 | … | | $W_1/W_n$ | $X_1=(1*(W_1/W_2)*…*(W_1/W_n))^{1/n}$ | ВАГА($A_1$) $=X_1/$СУМА($X_i$) |
| … | … | 1 | | $A_n$ | … | … |
| $A_n$ | $W_n/W_1$ | … | | 1 | $X_n=((W_n/W_1) *…*(W_n/W_{n-1}) *1)^{1/n}$ | ВАГА($A_n$)= $=X_n/$СУМА($X_i$) |
| | | | | | СУМА($X_i$) | |

Наступний крок: обчислення індексу узгодженості (ІУ), що дає інформацію про рівень порушення узгодженості.

$$\text{ІУ} = (L_{\max} - 1) / (n - 1)$$

де

$$L_{\max} = \sum_{i=1}^{n} S_i \cdot W_i,$$

$S_i$ – сума пріоритетів у стовпці,

$W_i$ – вага, записана у рядку.

Далі потрібно розділити отриманий індекс на параметр із спеціальної матриці випадкових індексів (ВІ) (табл. 3), яка була отримана експериментально.

Таблиця 3 – Випадкові індекси

| Розмір матриці | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Випадкова узгодженість | 0 | 0 | 0,58 | 0,9 | 1,12 | 1,24 | 1,32 | 1,41 | 1,45 | 1,49 |

Обчислюється відношення узгодженості (ВУ), як відношення ІУ та випадкового індексу ВІ для матриці:

$$ВУ = ІУ/ВІ.$$

Величина ВУ має бути близько 10% або менше, щоб бути прийнятною. У деяких випадках ВУ допускається до 20%, але не більше, інакше необхідна додаткова перевірка суджень, здійснених раніше.

Вирішимо задачу вибору копіювального апарату з використанням методу аналізу ієрархій.

Нехай на ринку є копіювальні апарати, закодуємо їх номерами N1, N2, N3, N4.

Задамо критерії оцінки та систему кодування:

А1 – Вартість апарату;

А2 – Підтримка копіювання документів формату А3 (так/ні – 0/1);

А3 – Швидкість копіювання (низька/середня/висока – 0/1/2);

А4 – Розмір (малий/середній/великий – 0/1/2);

Придумаємо чисельну систему порівняння якісних критеріїв.

Таблиця 4 – Параметри вибраних копіювальних апаратів та оцінка різниці для порівняння

| Параметри<br>Апарати | A1 | A2 | A3 | A4 |
|---|---|---|---|---|
| N1 | 200 | 0 | 0 | 0 |
| N2 | 200 | 0 | 1 | 0 |
| N3 | 500 | 1 | 1 | 1 |
| N4 | 800 | 1 | 2 | 2 |
| | Різниця-параметр | Різниця - параметр | Різниця - параметр | Різниця - параметр |
| | 0 – 1<br>100 – 3<br>400 – 5<br>700 – 7<br>900 – 9 | 0 – 1<br>1 – 3 | 0 – 1<br>1 – 3<br>2 – 5 | 0 – 1<br>1 – 3<br>2 – 5 |

Таблиця 5 – Оціка приоритетів

| | A1 | A2 | A3 | A4 | Добуток | Корінь | Вага | Si*Wi |
|---|---|---|---|---|---|---|---|---|
| A1 | 1 | 6 | 7 | 4 | 168 | 3,60 | 0,58 | 0,91 |
| A2 | 1/6 | 1 | 4 | 3 | 2 | 1,19 | 0,19 | 1,45 |
| A3 | 1/7 | 1/4 | 1 | 1/3 | 0,01 | 0,33 | 0,05 | 0,80 |
| A4 | 1/4 | 1/3 | 3 | 1 | 0,25 | 0,71 | 0,11 | 0,95 |
| Суми | 1,56 | 7,58 | 15,00 | 8,33 | | 5,83 | | 4,11 |

ИС=0,04
ОС=0,04

| A1 | | | | | | | |
|---|---|---|---|---|---|---|---|
| | N1 | N2 | N3 | N4 | Произведение | Корень | Значение |
| N1 | 1 | 1 | 4 | 6 | 24 | 2,21 | 0,36 |
| N2 | 1 | 1 | 4 | 6 | 24 | 2,21 | 0,36 |
| N3 | 1/4 | 1/4 | 1 | 4 | 0,25 | 0,71 | 0,11 |
| N4 | 1/6 | 1/6 | 1/4 | 1 | 0,01 | 0,29 | 0,05 |
| Суммы | 2,42 | 2,42 | 9,25 | 17,00 | | 5,42 | |

Рисунок 1– Результат обчислень А1

| A2 | | | | | | | |
|---|---|---|---|---|---|---|---|
| | N1 | N2 | N3 | N4 | Произведение | Корень | Значение |
| N1 | 1 | 1 | 3 | 3 | 9 | 1,73 | 0,28 |
| N2 | 1 | 1 | 3 | 3 | 9 | 1,73 | 0,28 |
| N3 | 1/3 | 1/3 | 1 | 1 | 0,11 | 0,58 | 0,09 |
| N4 | 1/3 | 1/3 | 1 | 1 | 0,11 | 0,58 | 0,09 |
| Суммы | 2,67 | 2,67 | 8,00 | 8,00 | | 4,62 | |

Рисунок 2 – Результат обчислень А2

| A3 | | | | | | | |
|---|---|---|---|---|---|---|---|
| | N1 | N2 | N3 | N4 | Произведение | Корень | Значение |
| N1 | 1 | 3 | 3 | 5 | 45 | 2,59 | 0,42 |
| N2 | 1/3 | 1 | 1 | 3 | 1 | 1,00 | 0,16 |
| N3 | 1/3 | 1 | 1 | 3 | 1,00 | 1,00 | 0,16 |
| N4 | 1/5 | 1/3 | 1/3 | 1 | 0,02 | 0,39 | 0,06 |
| Суммы | 1,87 | 5,33 | 5,33 | 12,00 | | 4,98 | |

Рисунок 3 – Результат обчислень А3

| A4 | | | | | | | |
|---|---|---|---|---|---|---|---|
| | N1 | N2 | N3 | N4 | Произведение | Корень | Значение |
| N1 | 1 | 1 | 3 | 5 | 15 | 1,97 | 0,32 |
| N2 | 1 | 1 | 3 | 5 | 15 | 1,97 | 0,32 |
| N3 | 1/3 | 1/3 | 1 | 3 | 0,33 | 0,76 | 0,12 |
| N4 | 1/5 | 1/5 | 1/3 | 1 | 0,01 | 0,34 | 0,05 |
| Суммы | 2,53 | 2,53 | 7,33 | 14,00 | | 5,04 | |

Рисунок 4 – Результат обчислень А4

Наводимо зведені оцінки за критеріями. Для отримання результатів необхідно для кожного апарату підсумувати нормалізовані критерії, помножені на свої ваги.

| | A1 | A2 | A3 | A4 | |
|---|---|---|---|---|---|
| | 0,91 | 1,53 | 1,16 | 0,81 | **результат** |
| N1 | 0,36 | 0,28 | 0,42 | 0,32 | **1,49** |
| N2 | 0,36 | 0,28 | 0,16 | 0,32 | **1,19** |
| N3 | 0,11 | 0,09 | 0,16 | 0,12 | **0,53** |
| N4 | 0,05 | 0,09 | 0,06 | 0,05 | **0,30** |

Рисунок 5 – Зведені результати

У результаті отримуємо, що потрібно вибрати копіювальний апарат N1. Наступний за перевагою апарат N2.

У ході виконання контрольної роботи розглянути метод аналізу ієрархій, який використовується при обґрунтуванні управлінських рішень при розробці та впровадженні систем менеджменту інформаційної безпеки та вирішено задачу вибору копіювального апарату.

# КІБЕРЗЛОЧИННІСТЬ

**Юрлакова І.,** ст. гр. Е-11-21, доц. Фастовець В.І.
ХНАДУ

Сучасний світ фактично нема як уявити без нових інформаційних технологій, в основі яких лежить широке застосування комп'ютерної техніки та новітніх засобів комунікацій. Зараз комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією.

Останнім часом в Україні значно зросла чисельність Інтернет користувачів, адже підключення до глобальної мережі стало доступним та зручним. Сьогодні особистий комп'ютер, КПК, мобільний телефон з підключенням до Інтернету сприймається наче належне та необхідне.

Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, змога проведення банківських, торгових, біржових операцій, переказування коштів і пребагато іншого. Інтернет – це чудовий засіб для зв'язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються, злочини, кіберзлочини.

На сьогоднішній день комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань . Стрімко збільшуються показники розповсюдження цих злочинів, а також без перерви зростає їх суспільна небезпечність. Це зумовлено прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосовування комп'ютерної техніки.

Треба зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив не підпорядкований розділ про ці злочини - розділ XVI «Злочини у сфері застосування електронно-обчислювальних машин

(комп'ютерів), систем та комп'ютерних мереж»; двократно положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві.

Кіберзлочинність - це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера, у якому перебувають дані про особ, приладдя, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а заразом іншого носія, навмисне призначеного для їхнього зберігання, обробки й передачі.

Родовим об'єктом злочинів, передбачених у розділі XVI КК України, є одиниця інформаційних відносин, які можливо визначити як інформаційні взаємини, засобом забезпеки яких є ЕОМ, системи, комп'ютерні мережі та мережі електрозв'язку.

По-іншому кажучи, злочини, передбачені цим розділом, посягають на певну частину інформаційних відносин – інформаційні відносини, які пов'язані із застосуванням спеціальних технічних засобів. У чинному кримінальному законі зараз наведено чотири види таких засобів:

- ЕОМ (комп'ютер) – функціональний пристрій, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв та може здійснювати розрахунки без участі людини;
- автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, котрий здійснює цю діяльність;
- комп'ютерна сітка – комплекс територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне користування цих ресурсів;
- телекомунікаційна мережа (мережа електрозв'язку) – комплекс технічних засобів телекомунікацій і споруд, призначених для маршрутизації, комутації, передавання та/або затвердження знаків, сигналів, письмового тексту, зображень і звуків чи повідомлень будь-якого роду

за допомогою радіо, проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням.

Відповідно до Конвенції про кіберзлочинність, яка є частиною українського законодавства з 11.10.2005 р., кіберзлочини умовно поділяються на чотири види.

Перший вид. До цього виду належать правопорушення супроти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

Сюди можна віднести всі злочини, спрямовані против комп'ютерних систем і даних (наприклад, нарочитий доступ до комп'ютерної системи або її частини; свідоме пошкодження, знищення, погіршення, модифікація або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продажу, здобуття для використання, поширення або надання для застосування іншим чином пристроїв, включаючи комп'ютерні програми).

Другий вид. До другого виду кіберзлочинів відносять правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрачання майна іншої особи в наслідок будь-якого введення, зміни, знищення чи приховування комп'ютерних даних чи будь-якого вторгнення у роботу комп'ютерної системи, з шахрайською або нечесною метою придбання не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид. Цей вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій з приводу вироблення, пропонування або надання доступу, поширення дитячої порнографії, а також володіння такими файлами у своїй системі кіберзлочинів охоплює правопорушення, пов'язані зі змістом, який полягає у здійсненні умисних незаконних дій стосовно вироблення, пропонування чи то надання доступу, поширення дитячої порнографії, а заразом володіння такими файлами у своїй системі.

Четвертий вид. Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, згідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про

торговельні аспекти прав інтелектуальної власності та Угоди BOIB про авторське право, а заразом національного законодавства України.

В Україні політика з приводу кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи.

Хакери мають значні можливості, щоб скористатися вразливістю кібербезпеки та досягти своїх злочинних цілей. На нинішній день можна виділити такі основні (найпопулярніші) способи:

• Фішинг – один з видів інтернет-шахрайства, коли «жертві» надсилаються сповіщення від імені відомих компаній або організацій одначе у дійсності вони не є справжніми. задум фішингу – отримання доступу до конфіденційних даних користувачів (паролів, логінів, даних особових рахунків і банківських карт). Зазвичай використовується метод проведення масових розсилок від імені популярних компаній або організацій, які містять посилання на фейкові сайти, які важко зовні відрізнити від справжніх. У листах особу ввічливо просять оновити чи підтвердити правильність персональної інформації чи то інформують про які-небудь проблеми з даними, а після цього перенаправляють на підроблений сайт, де треба ввести облікові дані. коли «жертва» вводить особисті дані на таких сайтах, то злочинцям стають відомі ці відомості та вони можуть використати їх з метою крадіжки персональних даних, персональних коштів або іншого. Фішинг є одним з найпоширеніших видів кібератак.

• Вірус – це програма, яка встановлюється без відома та проти волі користувача на його комп'ютер чи інакший пристрій. Комп'ютерний вірус можна «схопити» по-різному. Скажімо, вебсторінки та поштові вкладення можуть застосовуватися для безпосереднього запуску вірусу в систему. Зчаста вірус буває вбудований у завантажену з інтернету програму, яка «випускає» вірус на волю, пізніше як «жертва» її встановлює. Після зараження вірусом програма може заблоковувати доступ до файлів та системи з метою отримання

викупу. При цьому сплата викупу не завжди гарантує відновлення роботи системи.

• Соціальна інженерія – це підхід до злому, який не залежить від технологій і полягає у застосуванні шахраями тактики, завдяки якій вони переконують «жертву» розкрити конфіденційну інформацію. Тактики можуть бути різними: від видавання себе за співробітника банку, знайомого або товариша до різноманітних погроз із вимогою встановити шкідливе ПЗ.

• Шкідливе ПЗ (Malware) – до таких програм належать так звані «трояни», програми-шпигуни чи рекламне ПЗ. Достатньо часто вони встановлюються разом з іншою, корисною програмою, яку вирішила завантажити «жертва». Такі програми можуть таємно записувати всі натискання на клавіші, сканувати файли на жорсткому диску і читати cookie-файли браузера.

• Злам – це умисна дія, спрямована на несанкціоноване проникнення у ПЗ або систему шляхом обходу механізму безпеки, з метою отримання несанкціонованого доступу до певного ПЗ або системи.

• Вішинг – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком).

• Скімінг – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують міні-камери або змінні клавіатури.

• Шимінг – модернізований різновид скімінгу. У цьому разі шахраї використовують майже непомітний прилад, який розміщують усередині картридера. Таким чином дані кредитки копіюються непомітно.

• Онлайн-шахрайство – фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв’язку.

• Піратство – протиправне розповсюдження об’єктів інтелектуальної власності в Інтернеті.

• Мальваре – створення та поширення вірусів і шкідливого програмного забезпечення.

• Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.

• Рефайлінг – незаконна підміна телефонного трафіку.

Таким чином, кіберзлочинність – це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє зростати та поглинати дедалі більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи достатки порушників та зменшуючи вміст кишень пересічних громадян. Через те сьогодні насамперед важливо переглянути усі існуючі кроки та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

# ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

**Шагун Є.**, ст. гр. ЕА-11-21
ХНАДУ

Розвиток штучного інтелекту розпочинається у XVI столітті, коли Леонардо да Вінчі вперше спробував сформувати техніку для лічби. А вже у 1623 році німецький вчений Вільгельм Шікард сконструював автоматичний цифровий обчислювальний механізм, пізніше Блез Паскаль винайшов першу у світі обчислювальну техніку.

Створений розум полягає у здатності цифрового механізму брати, аналізувати та використовувати набуту інформацію та навички. Головною задачею його існування спочатку було допомогти людям з певною роботою, спростити її або зовсім замінити, заощадивши при цьому час.

Банківські підприємства використовують системи штучного інтелекту у діяльності страхування при участі на біржі та розпорядженні майном.

Наприкінці літа у 2001 році роботи здобули перемогу над людьми в торговому конкурсі на імпровізацію. Методики впізнавання фігур, широко застосовуються в оптичному та акустичному розпізнаванні (у тому числі текстовому та голосовому), медичній діагностиці та ін. ШІ займає значне положення в розробці планових способів доповнення реальності. А саме, ШІ сприяє проводженню класифікації та семантичної сегментації образів, локалізації та розпізнаванню мобільності предметів, щоб планово відтворювати контури елементів як символи повної реальності. Перспективна сфера використання ШІ – дослідження, в котрих буде відбуватися аналіз наукових статей для отримання нової інформації, знаходження невідомих матерій, закономірностей та іншого. За допомогою алгоритмів автоматизованого знаходження нової інформації на основі штучного розуму вдалося знайти майже 50 невідомих раніше екзопланет.

Найважливішими задачами вчених сьогодні вважають винайдення моделі мозку, відкриття загадок процесів мислення і свідо-

мості. У наш час є розумні машини, які вміють уявляти, спілкуватись, сміятися. Вона перший людиноподібний робот – Софія, добре розроблена конструкторами модель людини робота. Вона була створена у 2015 році гонконзькою інженерно-робототехнічною компанією Hanson Robotics, яка призначена розробці механізмів зі штучним інтелектом.

Софія приймала участь у праці ООН, може консультувати в сфері банків її національність Саудівська Аравія. На думку її творця роботи особливо корисні в сьогодення, в час, коли населення страшенно самотні та суспільно ізольовані. Залізна людина Софія – це перший головний прорив суспільства в подальше майбутнє, в якому машини, швидше за все, житимуть поряд з нами, їх створення безперечно буде спрощувати нам існування, або змінить його на гірше.

На думку Д. Генсона роботи все ж допомагатимуть людям, робитимуть наше життя простішим, легшим, взявши на себе більшу частину обов'язків, тоді як відомий вчений, фізик-теоретик Стівен Хокінг вважає, що винайдення роботів з незалежними процесами міркування становить насамперед загрозу для людського існування. Ілон Маск також закликає дослідницький світ бути обережними щодо такого несподівано швидкого кроку в розвитку штучного інтелекту.

Наразі штучний інтелект має безліч переваг. Першою розглянемо діагностику захворювань. За результатами дослідження, яке проводила аналітична компанія Global Market Insights, було визначено, що в наступні два роки на 40% щорічно збільшуватиметься застосування штучного інтелекту у сфері охорони здоров'я. Можливості ШІ вже зараз використовуються в діагностиці хвороб, вивченні геному, розробці лікарських засобів. Вони дозволяють надавати більш якісну інформацію, обслуговувати хворих, пацієнтів, зберігати час і гроші.

Ще одною перевагою є вивчення та аналіз великих обсягів інформації в усіх галузях економіки, промисловості, та інших областях. Досі ніхто з людей не здатен отримати, проаналізувати та видати правильне рішення так само швидко і чітко, як штучний інтелект. Наступна перевага – допомога можливостей штучного інтелекту в науці та космосі. Вчені винайшли віртуальних розумних

асистентів та назвали їх Cimon, щоб допомогти астронавтам. У небезпечних місцях, де людина фізично не може знаходитись дуже зручно використовувати технології штучного розуму. Останньою перевагою, але не за значенням є ефективність та економія у банківській області.

За допомогою можливостей штучного інтелекту можна запобігти шахрайство в банківському секторі, а також він допомагає в розробці політики інвестицій. У банках використовуються програми на основі ШІ за допомогою яких можна запобігти відмиванню грошей.

Крім переваг штучний інтелект має й деякі можливі загрози, а саме: масове безробіття, можливість втрати контролю над штучним розумом. Можливе створення конфліктів на, соціальному, економічному, релігійному рівнях. Штучний інтелект може допомогти в досягненні нової науково-технічної революції, але може і стати загрозою людства. Через те що він забезпечує суспільство усіма необхідними елементами для життя, воно стає більш вразливим і залежним.

У сучасному світі де важливими навичками є швидкість обробки інформації, що стрімко надходить, ефективність розподілення ресурсів штучний інтелект істотно полегшує життя. Він не замінює людину, він спрощує її роботу.

Зараз він вже активно використовується в автоматизації – участь людей в процесах, що добре функціонують зведена до мінімуму, в аналізі даних – штучний інтелект зовсім не втомлюється і набагато менше помиляється, коли необхідно обробляти великі обсяги даних. Також роботи можуть збирати механізми з різних деталей, класифікувати, вивчати, та тестувати. Існують розумні машини, які можуть проаналізувати поведінку робітника на робочому місці та запобігти нещасним випадкам.

За допомогою різних датчиків руху і камер системи можуть стежити за порядком в місцях багато скупчення людей та на вулицях. Чиновники використовують технології штучного інтелекту в роботі, чим суттєво скорочують час використаний на систематизацію та опрацювання документів, патентів, ліцензій. Вони допомагають швидко збирати та обробляти дані, за допомогою яких лікарі швидше

і точніше ставлять діагноз. В медицині вже зараз розумні програми використовуються для діагностики, досліджень онкології, прогнозування захворювань генетики, серцево-судинними хворобами.

Штучний інтелект допомагає, у підборі кандидатів на робочі місця та у зведенні потенційних роботодавців і співробітників. Найпопулярнішим продуктом, створеним за допомогою технологій ШІ є смарт-хаус, або розумний будинок. У повсякденності нам допомагають і портативні пристрої, а саме фітнес-браслети, розумні смарт-годинники і таке інше. Веб-аналіз даних користувачів соціальних мереж, щоб визначити потреби та інтереси виконується функціями ШІ.

Створення колекцій фільмів, музичних продуктів на основі зібраних даних. Основні сфери застосування цих засобів пов'язані з підтримкою прийняття управлінських рішень у таких сферах бізнесу, як кредитування та оцінка ризиків, маркетинговий аналіз, прогнозування фінансового ринку, моделювання функціональних компонентів управління тощо.

Як приклад застосування можливостей штучного інтелекту в житті можна взяти чат-боти вони вміють розпізнавати фрази та слова для аналізу та надавання потрібної корисної інформації клієнтам які ставлять запитання загального характеру. Інколи здається що розмовляєш з реальною людиною через високу точність чат-ботів. Вони намагаються імітувати справжню мову, коли допомагають у звичайних завданнях, наприклад бронювання зустрічей, відповіді на питання або приймання замовлень.

Музичні рекомендації, рекомендації щодо товарів виконуються за допомогою розумного пошуку Google. Для запобігання фінансового шахрайства на мобільний телефон механізми ШІ відправляють сповіщення. Наприклад якщо по вашій банківський карті відбувається незвично велика транзакція можна отримати SMS-попередження. Або якщо раптом ви почнете щось купувати іншій державі, вам прийде повідомлення яке буде вимагати зателефонувати до свого банку для особистого підтвердження покупки. Надходження цих повідомлення можливе завдяки щоденному відстеженню фінансових транзакцій, які ви проводите. Це дозволяє штучному інтелекту розпізнавати незвичайні ситуації у ваших витратах. Коли такі

програми як Google Maps прокладають найшвидший шлях до місця призначення, обчислюють і аналізують трафік, ремонт доріг, тобто допомагають в навігації – це ШІ в дії.

Восени 2017 року компанія Facebook почали виконання функції виявлення, її сенс у скануванні повідомлень та виявленні дій, які можуть вказувати на те, що користувач думає про самогубство. Коли система Facebook виявляє у користувача подібні суїцидальні думки, програма на основі ШІ надсилає дані про психічне здоров'я самому користувачеві, а інколи й друзям. У 2015 році було проведено опитування серед льотчиків авіакомпанії Boeing 777 його результати повідомили що на керування літаком, під час звичайного польоту пілот витрачає лише 7 хвилин, решта часу – більша частина пілотування виконується механізмами штучного інтелекту. Існує ще дуже багато прикладів програм на основі ШІ котрі допомагають нам робити різні повсякденні речі, наприклад навіть спілкування з друзями, родичами за допомогою використання програми електронної пошти або сервісу ride-share.

Розробка та запровадження ШІ, безумовно, є важливим кроком у переході до новітніх технологій, розвитку та наукового майбутнього. Як результат всього вищезгаданого можна впевнено сказати що штучний інтелект робить наше життя ефективнішим. І якщо у вас ще залишились деякі застереження щодо використання штучного інтелекту, можливо вас заспокоїть те, що багато з нас використовує допомогу ШІ щодня вже протягом багатьох років.

УДК 378.147:004

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМІ СУЧАСНОЇ ОСВІТИ

**Костікова М. В. [1], Бугай А. В. [2]**
*[1] канд. техн. наук, доцент, [2] студентка групи МК-11-21,*
ХНАДУ, м. Харків, Україна
E-mail: [1] kmv_topaz@ukr.net, [2] bugayalbina9@gmail.com

Сучасні технології в освіті дозволяють отримувати знання дистанційно, у більш повному обсязі та з меншими витратами часу та грошей. З'явилися нові способи взаємодії між викладачем та студентом. При виборі навчального закладу акцент змістився на якість навчання, а не на близькість до місця проживання.

Інтернет вніс корективи до освіти. Зміни торкнулися як методів навчання, і підходів до організації освітнього процесу. Система освіти проходить етап злиття із загальносвітовим інформаційним простором. Це дозволяє використовувати сучасні способи вивчення матеріалу, які стають зручнішими та доступнішими. Технічні пристрої – основа процесу модернізації у системі освіти. З їхньою допомогою можна якісно вивчати матеріал без прив'язки до місця занять.

Дистанційні технології в освіті дозволяють взаємодіяти студентам та викладачам незалежно від місця проживання. Для цього проводять: вебінари; онлайн-зустрічі в месенджерах та сервісах; практику в сучасних комп'ютерних кабінетах; доступ до особистих кабінетів на сервісах платформ навчання.

Традиційні методи навчання спрямовані на механічне запам'ятовування інформації. При цьому не враховується зручність перебування у навчальному кабінеті. В результаті інформація передається стандартно, не торкаючись мультимедійних та інших способів взаємодії зі студентами. Навчання у форматі онлайн дозволяє швидше знаходити актуальну інформацію з теми, що вивчається. Якщо навчання за допомогою комп'ютерів та інших пристроїв відбувається

у сучасному кабінеті, студенти можуть отримувати знання за більш зручніших умов.

Замість застарілих підручників використовується база даних, що оновлюється. Також для віддалених занять створюють зручне середовище, що включає комп'ютери, інтерактивні дошки та ін.

Якщо електронне навчання дистанційним способом можливе з дому, учні можуть отримувати знання без відвідування навчальних аудиторій. Це також впливає на якість засвоєння матеріалу. Заняття в домашніх умовах відмінно пасує людям, які мають проблеми із соціумом.

Зараз техніка та інформація є фундаментом для вивчення наук, налагодження виробництва та поліпшення життя. Вплив сучасних технологій на освіту виявився вирішальним для його розповсюдження. Це спричинило те, що цінується не сама інформація, а вміння її знайти.

Зросла важливість знання комп'ютерних програм, систем та сервісів. Використання сучасних систем дозволило звести до мінімуму ймовірність похибки та людського фактора. Сучасні інформаційні технології дозволили в короткий термін надати доступ до знань практично всьому соціуму.

Це стало можливо завдяки зменшенню фізичних розмірів обчислювальних модулів і процесорів. Доступність Інтернету, комп'ютерів та способів навчання дозволяє підвищити загальний рівень грамотності населення. Здешевлення виробництва обчислювальної техніки також впливає на зростання затребуваності дистанційного навчання.

З 2020 року у світі активно поширився коронавірус – COVID-19. Безліч країн запровадило обмеження для проведення масових заходів, заборона відвідування місць скупчень людей. Запроваджено дистанційні форми навчання у школах, вузах та інших організаціях. Незважаючи на це, дистанційні технології в освіті дозволили цій сфері зміцнити позиції.

Внаслідок заборон та ризику придбати інфекцію при спілкуванні з людьми, багато хто перейшов на навчання за допомогою Інтернету. Школи, вузи та центри в короткий термін змінили способи навчання або покращили існуючі дистанційні курси. Стандартні програми

освіти було змінено під інтерактивний формат. Тепер інформацію можна отримати не лише очно, а й за допомогою Інтернету.

Ряд університетів України до 2020 року вже ввели нові системи викладання, тому пандемія лише підштовхнула багато університетів та освітніх центрів до природних змін у більш короткий термін.

Електронне навчання та дистанційні курси дозволяють підвищити кваліфікацію та рівень знань спеціалістів різних сфер діяльності. При цьому на підготовку йде менше часу.

Віддалені курси – це можливість знайти відповідний навчальний заклад не лише у своєму місті, а й по всій Україні чи навіть у світі. Тому курси та програми навчання більш престижних організацій стають доступнішими.

Тепер кваліфікованим спеціалістам достатньо використати дистанційні технології в освіті.Процес навчання за допомогою Інтернету розвивається швидко. Проте чи всі викладачі готові змінити звичний спосіб роботи більш просунутий. Електронне навчання та дистанційні методи подачі матеріалу повинні розвинути потребу у знанні.

Повне обмеження живого спілкування, залежність від соціального схвалення та відсутність можливості висловитись – усе це може призвести лише до негативних наслідків такої системи. Якщо електронна освіта не має структури, а пропонується лише як необов’язкове доповнення – якість навчання страждатиме.

Переваги сучасних технологій для освіти: навчання у зручному місці; стимулювання до самоосвіти; швидкий та простий пошук інформації; відсутність територіальної прихильності; покращення знань щодо способів використання інформаційних технологій; доступ до інформації не обмежується літературою навчального закладу тощо.

Інтелектуальний рівень та здатність до самонавчання підвищується при використанні телекомунікаційних технологій. Це сприятливо впливає на освіту людей, допомагає навчитися самодисципліни та правильно шукати інформацію для майбутньої роботи.

Електронне навчання та дистанційні курси допомагають старшому викладацькому складу вивчати нові та змінювати звичні способи навчання. В результаті можна покращити систему навчання,

в якій поєднуватимуться практичні навички досвідченого педагога та нова теоретична інформація про напрямок діяльності.

Використання комп'ютера для ознайомлення із матеріалом розвиває абстрактне мислення. Для цього використовуються відеоролики, аудіофайли, презентації та багато іншого.

Розглянемо нові впровадження в сучасну освіту.

*Віртуальна та доповнена реальність.* Візуальні засоби та технології дедалі більше використовуються в освітньому процесі. Справа, знову ж таки, в особливостях нинішнього покоління. Статистика показує, що YouTube постійно використовують 85% підлітків, при цьому 80% із них стверджують, що відео для них – спосіб дізнатися більше про свої хобі. Не дивно, що викладачі все частіше використовують у навчанні відеоматеріали, фільми та записані лекції.

З розширенням використання сучасних освітніх технологій студенти зможуть вивчати предмети за допомогою технологій віртуальної та доповненої реальності. Наприклад, одягнувши VR-шолом, студент зможе спостерігати історичні події та навіть брати участь у них. Таке навчання називається іммерсивним, воно створює «ефект присутності» і дозволяє переживати неможливий у світі досвід. Такий захоплюючий сучасний формат навчання дозволить якісніше засвоювати інформацію.

Ми все ще чекаємо, що доповнена реальність штормом пройдеться у нашому світі.

*3D-принтер.* Юні інженери та їх викладачі – найкращий приклад людей, які потребують 3D-друку під час навчання. 3D-принтер дозволяє створити робочу міні-модель, щоб перевірити інженерну конструкцію, тому студенти можуть відточити свої навички до дрібниць. Сьогодні, володіючи програмами CAD, будь-який студент може заощадити багато часу і грошей, якщо доповнить своє обладнання 3D-принтером. Крім того, фізичні моделі розвивають абстрактне мислення, отже, якщо роздрукувати фізичну версію структури, школярі зможуть краще зрозуміти, з чим мають справу.

*Хмарні обчислення.* Хмарні технології розвиваються, і дуже скоро всі без винятку аспекти нашого життя, у тому числі й освіта, будуть схильні до змін. В аудиторіях майбутнього студентам просто знадобиться електронний пристрій, який надасть доступ до

домашньої роботи та інших навчальних ресурсів у хмарі. Жодних важких підручників, всі матеріали будуть доступні доти, доки є з'єднання з Інтернетом. Така зручність надасть студентам певної свободи, адже можна працювати над проектами як удома, так і в будь-якому іншому місці. Хмарні обчислення прагнуть віртуалізувати класну кімнату.

Вищі навчальні заклади можуть використовувати хмарні технології та створювати онлайн-платформи для навчання студентів. Досить просто увійти до системи та відвідувати заняття у віртуальному середовищі.

---

Наприклад, концепт хмарного віртуального середовища навчання (VLE), яке дозволяє студентам отримати доступ до навчального контенту та брати участь у обговореннях на форумах. Завдання або тести легко можна розповсюджувати по всьому класу, зводячи до мінімуму необхідність бути фізично присутніми студентам, але заохочуючи взаємодію та обговорення; вчителям буде відведено інший канал.

*Соціальні мережі онлайн.* Численні університети вже реєструвалися у віртуальному світі Second Life, щоб надати студентам онлайн-платформу для спілкування один з одним. Будучи великою частиною хмарної платформи, такі соціальні мережі дозволяють студентам зосередитися на навчанні та вільно обговорювати ідеї, тоді як вчителі будуть виступати у ролі модераторів.

Важлива роль у цьому відводиться викладачам і професорам, які можуть виступати у ролі керівництва, допомагаючи з відповідями й запитуючи, моментально завантажуючи інформацію у хмарне середовище. Ще одна перевага в тому, що вона є відмінним інструментом зворотного зв'язку. Соціально-орієнтований підхід у навчанні у майбутньому може стати основою.

*Біометрія: відстеження очей.* Ще одна технологія, яка швидко завойовує визнання, – це біометрія. Умовно біометрію зазвичай пов'язують із сферою безпеки, оскільки вона використовує те, що є унікальним для кожного з нас: відбитки пальців, розпізнавання облич, голоси, сітківки ока. З точки зору освіти, установа могла б використовувати відбитки пальців для запобігання прогулам і видачу книг з бібліотеки.

---

Тим не менш, відстеження очей також може бути корисним, наприклад, тим, що надає безцінну інформацію для викладачів. Це ж наочне зображення того, як студент поглинають інформацію та розуміють зміст. У рекламі ці дослідження допомагають визначити, як користувачі реагують на оголошення і що безпосередньо заволодіває їх увагою. Аналогічним чином цю форму аналізу можна використовувати для з'ясування ефективності курсу чи стилю навчання. Наприклад, використовується S2 Eye Tracker, щоб оцінити якість навчання студентів за рахунок того, куди вони дивляться під час занять.

Дані можуть бути організовані таким чином, щоб кожному з студентам було зручно, тобто відповідно до його стилю навчання. З іншого боку, моделі руху очей також можуть визначати постачання контенту та виявляти проблеми до того, як вони виникнуть. Наприклад, у неправильній подачі матеріалу.

*Мультитач-дисплеї.* За останні кілька десятиліть багато хто побачив появу відеопроекторів у школах, а також перехід від звичайної крейдової дошки до білої дошки. Цілком можливо, наступним кроком буде щось, пов'язане зі смартфонами та планшетами. Наприклад, наступна «дошка» може стати гігантським сенсорним РК-екраном, що дозволяє велику інтерактивність. Основна відмінність між нашими нинішніми сенсорними пристроями та такою дошкою буде в тому, що вона дозволить введення даних одразу від кількох учнів.

---

І замість традиційної дошки в класі цілком можливо гігантський планшет у формі столу. Студенти або учні можуть сидіти навколо такого столу-планшета, працювати з вмістом та перетягувати зображення так само просто, як робити нотатки за допомогою віртуальної клавіатури.

Головна мета інноваційної освіти – збереження і розвиток творчого потенціалу людини.

Система освіти в Україні є однією з важливих конкурентних переваг нашої держави. Саме сучасна освіта формує майбутнє країни, перспективи її розвитку в довгостроковій перспективі. Суспільний прогрес, розвиток економічних та політичних інститутів прямо

впливають на освітню сферу. Від того, на скільки оперативно система освіти реагує на зміни, залежить її ефективність.

Сучасна освіта – це відхід від традиційних класичних форм із переходом на платформу інформаційних мереж, зокрема, Інтернет. Сьогодні на порядку денному дистанційна сучасна освіта.

Сьогодні реформа здійснюється за такими пріоритетними напрямами: доступна та якісна дошкільна освіта; нова українська школа; сучасна професійна освіта; якісна вища освіта та розвиток освіти дорослих; розвиток науки та інновацій.

Таким чином, ми бачимо, що сучасний період розвитку суспільства характеризується сильним впливом комп'ютерних технологій, які проникають у всі сфери людської діяльності, забезпечують поширення інформаційних потоків у соціумі створюючи глобальний інформаційний простір. Невід'ємною і важливою складовою цих процесів є комп'ютеризація освіти.

УДК 004.056.5

# КОМП'ЮТЕРНА БЕЗПЕКА – ЦІЛІСНІСТЬ ДАНИХ І КОНФІДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ

**Костікова М. В. [1], Гетало Д. І. [2], Гура В. О. [3]**
*[1] канд. техн. наук, доцент, [2, 3] студенти групи ДМ-21-20*
*ХНАДУ, м. Харків, Україна*
E-mail: [1] kmv_topaz@ukr.net, [2] getalo30@gmail.com, [3] torriaaa007@gmail.com

Кожного дня хакери піддають загрозі багато ресурсів, стараючись здобути до них доступ. Цьому сприяють два основні фактори. По-перше, це повсюдне проникнення Інтернет. Зараз до мережі Інтернет приєднані мільйони пристроїв. Багато пристроїв будуть приєднані до неї в майбутньому.

Отже ймовірність доступу хакерів до уразливих пристроїв безперервно зростає. Крім того, широке розповсюдження Інтернет позволяє хакерам обмінюватися інформацією в глобальному масштабі. По-друге, це спільне поширення простих у застосовуванні операційних систем і оточень розроблення. Цей чинник різко знижує рівень знань і досвід, які необхідні хакеру.

Мережеві атаки настільки ж різні, як і системи, проти яких вони спрямовані. Деякі атаки різняться складністю. Інші може здійснити простий користувач, навіть не здогадуватися, які наслідки може мати його діяльність. Для оцінки різновидів атак необхідно знати окремі обмеження, спочатку властиві протоколу TCP / IP. В умовах ранніх версій Інтернет-протоколу (IP) були неприсутні вимоги безпеки. Саме тому багато реалізації IP є передусім уразливими. Згодом стали запроваджувати засоби безпеки для IP.

Однак з огляду на те, що спершу способи захисту для протоколу IP не розроблялися, всі його реалізації стали доповнюватися всілякими мережевими процедурами, послугами та продуктами, що знижують загрози, властиві цим протоколом. Далі розглянемо типи атак, які застосовуються проти мереж IP, і перерахуємо способи боротьби з ними.

1. Сніфери пакетів (перехоплення та аналізу мережевого трафіку сторонніми особами).

Основними методами захисту від сніфінгу є:

- аутентифікація;
- комутована інфраструктура;
- антисніфери;
- криптографія.

*Автентифікація*. Міцні засоби автентифікації є першим способом захисту від сніфінга пакетів. Під «міцним» ми розуміємо такий метод автентифікації, який тяжко уникнути. Зразком такої автентифікації є одноразові паролі. Якщо хакер узнає цей пароль за допомогою сніфер, ця інформація буде даремна, тому що в цей момент пароль вже буде використаний і виведено з ужитку.

*Комутована інфраструктура.* Якщо, для прикладу, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіка, що приходить на той порт, до якого вони підключені.

*Антисніфери.* Полягає в установці апаратних чи програмних засобів, які розпізнають сніфери, які працюють у вашій мережі. Вони включаються в загальну систему захисту. Антисніфери замірюють час реагування хостів і визначають, чи не доводиться хостам обробляти «зайвий» трафік.

*Криптографія*. Дієвий засіб боротьби зі сніфінгом пакетів не запобігає перехоплення і не розпізнає роботу сніфера, але робить цю роботу марною. Якщо канал зв’язку є криптографічно захищеним, це значить, що хакер підхоплює не повідомлення, а зашифрований текст.

2. IP-спуфінг.

IP-спуфінг виникає, коли хакер, що перебуває усередині корпорації або поза її, видає себе за санкціонованого користувача. Це можна зробити двома способами. По-перше, хакер може застосувати IP-адресу, або вповноважити зовнішню адресу, якій дозволяється доступ до певних ресурсів мережі. Атаки IP-спуфінга часто є первинною точкою для інших атак. Зазвичай обходиться вставкою неправильної інформації або шкідливих команд у звичайний потік

даних. Для двобічного зв'язку хакер повинен переробити всі таблиці маршрутизації, щоб направити трафік на хибну IP-адресу. Якщо головне завдання полягає в отриманні від системи вагомого файлу, відповіді додатків не мають значення. Якщо ж хакеру удається змінити таблиці маршрутизації і направити трафік на неправильну IP-адресу, хакер отримає всі пакети і зможе відповідати на них так, ніби він є санкціонованим користувачем.

Загрозу спуфінга можна ослабити (але не усунути) за допомогою таких заходів:

*Контроль доступу*. Щоб знизити ефективність IP-спуфінгу, відрегулюйте контроль доступу на відсікання будь-якого трафіка, що надходить з зовнішньої мережі з вихідною адресою, який повинен влаштовуватися усередині вашої мережі. Якщо санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає недійовим.

*Фільтрація RFC 2827.* Ви можете припинити спроби спуфінга незнайомих мереж користувачами вашої мережі. Для цього варто відбраковувати будь-який вихідний трафік, початкова адреса якого не є однією з IP-адрес вашої організації. У наслідку відбраковується весь трафік, який не має вихідної адреси, очікуючого на певному інтерфейсі.

3. Відмова в обслуговуванні (Denial of Service – DoS).

DoS – найбільш відома форма хакерських атак. Проти атак подібного типу найважче створити стовідсотковий захист. Атаки DoS різняться від атак інших типів. Атака DoS робить вашу мережу недоступною для простого використання викликано перевантаження мережі, функціонування мережі, програми або операційної системи.

Існує три способи зниження загроз DoS атак.

*Функції анти-спуфінга.* Ці функції, як мінімум, зобов'язані включати фільтрацію RFC 2827. Якщо хакер не зможе затаїти свою справжню особистість, він навряд чи відважиться провести атаку.

*Функції анти-DoS.* Ці функції нерідко лімітують кількість напіввідкритих каналів у будь-який момент часу.

*Обмеження обсягу трафіка.* Організація може попрохати провайдера (ISP) обмежити обсяг трафіка.

4. Парольні атаки.

Хакери вміють проводити парольні атаки за допомогою великого ряду методів, таких як простий перебір, «троянський кінь», IP-спуфінга і сніфінг пакетів. Одноразові паролі або криптографічна аутентифікація практично зводять такий тип загроз.

5. Атаки типу Man-in-the-Middle.

При атаки типу Man-in-the-Middle хакер отримує доступ до пакетів, що передаються по мережі. Атаки проводяться з метою крадежу інформації, перехоплення поточної сесії і одержання доступу до часних ресурсів мережи. З атаками типу Man-in-the-Middle можна ефективно боротися тільки за допомогою шифрування.

6. Атаки на рівні додатків.

Атаки на рівні додатків можна провести різними засобами. Найпоширеніший з них полягає у вживанні добре визначних слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Вживаючи ці слабкості, зловмисники отримують доступ до комп'ютера від імені користувача, що зареєстровано в додатки.

Найбільша проблема з атаками на рівні додатків полягає в тому, що вони часто використовують порти, які мають доступ для проходу через міжмережевий екран. Наприклад, хакер, який експлуатує відому слабкість Web-сервера, найчастіше використовує для атаки TCP порт 80. Оскільки Web-сервер дозволяє користувачам Web-сторінки, міжмережевий екран зобов'язаний надавати доступ до цього порту.

Повністю виключити атаки на рівні додатків неможливо. Головне тут – хороше системне адміністрування.

7. Мережева розвідка.

Мережева розвідка – це збір інформації про мережу за допомогою доступних даних і додатків. Для мережевою розвідки використовується запити DNS, сканування портів і exo-тестування. DNS запити дозволяють отримати інформацію, про власника того чи іншого домену і які адреси цього домену привласнені. Exo-тестування адрес, розкритих за допомогою DNS, дозволяє дізнатися,

які хости дійсно роблять у даному середовищі. Діставши список хостів, хакер вживає засоби сканування портів, для складання повного списку послуг, які надаються цими хостами. У результаті зловмисник отримує інформацію, яку може використати для взлому.

8. Зловживання довірою.

Власне кажучи, цей тип дій не є «атакою» або «штурмом». Він являє собою зловмисне вживання відносин довіри, що існують у мережі. Класичним зразком такого зловживання є ситуація в периферійній частині корпоративної мережі.

Ризик зловживання довірою можна знизити за рахунок більш грубого контролю ступенів довіри в межах своєї мережі. Відносини довіри повинні обмежуватися певними протоколами і, по можливості, аутентифікуватися не тільки по IP-адресам, а й за іншими параметрами.

9. Переадресація портів.

Переадресація портів є різновидом зловживання довірою, коли зіпсований хост використовується для передачі через міжмережевий екран трафіка, який в іншому випадку був би неодмінно відбракований. Зовнішній хост має можливість підключитися до хосту загального доступу (DMZ), але не до хоста, встановленого з внутрішньої сторони міжмережевого екрану. Хост загального доступу може підключатися і до внутрішнього, і до зовнішнього хосту. Якщо хакер загарбає хост загального доступу, він зможе встановити на ньому програмний засіб, що перенаправляють трафік з зовнішнього хоста прямо на внутрішній хост. Завадити хакеру приладнати на хості свої програмні засоби може хост-система IDS (HIDS).

10. Несанкціонований доступ.

Несанкціонований доступ не може прийматися окремим типом атаки. Більшість мережевих атак проводяться задля отримання несанкціонованого доступу. Щоб підібрати логін Telnet, хакер повинен спочатку отримати підказку Telnet на своїй системі. Після підключення до порту на екрані появлятиметься повідомлення. Якщо після цього хакер продовжить спроби доступу, вони будуть прийматися несанкціонованими.

Засоби боротьби з несанкціонованим доступом доволі прості. Головним тут є скорочення або повна знищення можливостей хакера з отримання доступу до системи за допомогою несанкціонованого протоколу.

11. Віруси і додатки типу «Троянський кінь».

Робочі станції фінальних користувачів дуже вразливі для вірусів і «Троянських коней». «Троянський кінь» – це не програмна вставка, а повноцінна програма, яка виглядає як благодійна програма, а на ділі здійснює шкідливу роль. Зразком типового «Троянського коня» є програма, яка виглядає, як звичайна гра, поки користувач грає у гру, програма поширює свою копію електронною поштою кожному абоненту адресної книги цього користувача. Кожен абонент одержує поштою гру, та може викликати її подальше поширення.

Для боротьби з вірусами та «Троянськими кіньми» використовується ефективні антивірусні програми забезпечення, які працюють на рівні користувача та на рівні мережі

Політика безпеки – це формальний набір правил, яким зобов’язані підкорятися працівники, які мають доступ до корпоративної технології та інформації.

Засоби мережі в себе включають:

- Хост мережі (персональні комп’ютери; включає операційні системи, програми, дані хостів).
- Пристрої мережі (маршрутизатори, міжмережеві екрани).
- Дані мережі (дані, які передаються з даної мережі).

Опорними елементами політики у галузі безпеки є ідентифікація, цілісність і активна перевірка. Ідентифікація запобігає загрозі знеособлення і несанкціонованого доступу до ресурсів і даних. Цілісність забезпечує захист від підслуховування і маніпулювання даними, підтримуючи конфіденційність і незмінність переданої інформації.

Активна перевірка (аудит) значитиме перевірку правильності виконання елементів політики безпеки.

Цілісність – це елемент, який включає захист пристрою інфраструктури мережі (логічний і фізичний доступ), безпеку периметра і конфіденційність даних. Безпека фізичного доступу може виражатися

в розстановці обладнання мережі в навмисне створених для цього оснащення шафах, які мають обмежений доступ.

Приватність даних може забезпечуватися протоколами безпеки на транспортному рівні SSL і Secure Shell Protocol (SSH), які виконують безпечну передачу даних між клієнтом і сервером.

Засіб SOCKS є рамковою будовою, що дозволяє додаткам клієнт / сервер в доменах TCP і UDP сприятливо і безпечно вживати послуги мережевого міжмережевого екрану.

Останнім визначним елементом системи безпеки є аудит, який портібний для стеження і верифікації процесу дослідження політики безпеки. Для випробування ефективності інфраструктури системи безпеки, аудит безпеки має відбуватися часто, через рівні інтервали часу. Він також зобов'язаний включати перевірки установки новітньої системи, методи для визначення можливих шкідницьких дій будь-кого з внутрішнього колективу і можливої присутності своєрідного класу проблем (нападу типу «відмова в сервісі»), а також суцільне дотримання політики безпеки об'єкта.

При розробленні політики безпеки необхідно враховувати вимогу збалансувати легкість доступу до інформації і ідентичний механізм ідентифікації дозволеного користувача і забезпечення цілісності та конфіденційності даних. Політика безпеки буде по-справжньому ефективна, якщо вона впроваджується примусово як технічно, так і організаційно.

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМІ СУЧАСНОЇ ОСВІТИ

Бугай А.В., ст.гр. МК-11-21,
керівник канд. тех. наук, доцент Костікова М.В.
ХНАДУ

## Вступ

Сучасні технології в освіті дозволяють отримувати знання дистанційно, у більш повному обсязі та з меншими витратами часу та грошей. З'явилися нові способи взаємодії між викладачем та студентом. При виборі навчального закладу акцент змістився на якість навчання, а не на близькість до місця проживання.

## Вплив інформаційних технологій на освіту

Інтернет вніс корективи до освіти. Зміни торкнулися як методів навчання, і підходів до організації освітнього процесу.

Система освіти проходить етап злиття із загальносвітовим інформаційним простором. Це дозволяє використовувати сучасні способи вивчення матеріалу, які стають комфортнішими та доступнішими.

Технічні пристрої (комп'ютери, смартфони, планшети тощо) – основа процесу модернізації у системі освіти. З їхньою допомогою можна якісно вивчати матеріал без прив'язки до місця занять.

Дистанційні технології в освіті дозволяють взаємодіяти студентам та викладачам незалежно від місця проживання. Для цього проводять:

- вебінари;
- онлайн-зустрічі в месенджерах та сервісах;
- практику в сучасних комп'ютерних кабінетах;
- доступ до особистих кабінетів на сервісах платформ навчання.

Традиційні методи навчання спрямовані на механічне запам'ятовування інформації. При цьому не враховується зручність перебування у навчальному кабінеті. В результаті інформація передається стандартно, не торкаючись мультимедійних та інших способів

взаємодії зі студентами. Електронна освіта та інформаційні технології дозволяють розширити можливості навчання людей.

Навчання у форматі онлайн дозволяє швидше знаходити актуальну інформацію з теми, що вивчається. Якщо навчання за допомогою комп'ютерів та інших пристроїв відбувається у сучасному кабінеті, студенти можуть отримувати знання за більш комфортних умов.

Замість застарілих підручників використовується база даних, що оновлюється. Також для дистанційних занять створюють зручне інформаційне середовище, що включає сучасні комп'ютери, інтерактивні дошки та ін.

Якщо електронне навчання дистанційним способом можливе з дому, учні можуть отримувати знання без відвідування навчальних аудиторій. Це також впливає на якість засвоєння матеріалу. Заняття в домашніх умовах відмінно підходить людям, які мають проблеми із соціалізацією.

Зараз техніка та інформація є фундаментом для вивчення наук, налагодження виробництва та поліпшення життя. Вплив сучасних технологій на освіту виявився вирішальним для його розповсюдження. Це спричинило те, що цінується не сама інформація, а вміння її знайти.

Також зросла важливість знання комп'ютерних програм, систем та сервісів.

Раніше креслення мали створювати, використовуючи ручні інструменти та власні знання. Зараз потрібні знання програм та технічного пристрою. Використання сучасних систем дозволило звести до мінімуму ймовірність похибки та людського фактора. Сучасні інформаційні технології дозволили в короткий термін дати доступ до знань практично всьому людству. Це стало можливо завдяки зменшенню фізичних розмірів обчислювальних модулів і процесорів. Наприклад, обчислювальні машини минулого століття не змогли б конкурувати з сучасними комп'ютерами через величезні розміри, але низьку потужність. У 1975 році Гордон Мур вніс корективи до «Закону Мура», згідно з яким подвоєння числа транзисторів відбуватиметься кожні два роки. Отже, розвиток потужностей комп'ютерів, мікрокомп'ютерів та інших пристроїв відбувається експонентно. Це не лише на швидкість обчислень, а й у вартість технічних пристроїв.

Таким чином, дистанційні технології в освіті стають дешевшими, а доступ до навчальних ресурсів з'являється у більшої кількості людей. Доступність Інтернету, комп'ютерів та способів навчання дозволяє підвищити загальний рівень грамотності населення. Здешевлення виробництва обчислювальної техніки також впливає на зростання затребуваності дистанційного навчання.

У 2020 році у світі активно поширився коронавірус – COVID-19. Безліч країн запровадило обмеження для проведення масових заходів, заборона відвідування місць скупчень людей. Запроваджено дистанційні форми навчання у школах, вузах та інших організаціях.

Незважаючи на це, дистанційні технології в освіті дозволили цій сфері вижити та зміцнити позиції. Внаслідок заборон та ризику придбати інфекцію при спілкуванні з людьми, багато хто перейшов на навчання за допомогою Інтернету.

Школи, вузи та центри в короткий термін змінили способи навчання або покращили існуючі дистанційні курси. Стандартні програми освіти було змінено під інтерактивний формат. Тепер інформацію можна отримати не лише очно, а й за допомогою Інтернету.

Електронна освіта та дистанційні технології дозволили людям підвищувати кваліфікацію, проходити професійну перепідготовку та короткострокове навчання без відриву від виробництва. Школярі та студенти також змогли не зупиняти навчання, а пристосуватися до нових способів отримання інформації.

Ряд університетів України до 2020 року вже ввели нові системи викладання, тому пандемія лише підштовхнула багато університетів та освітніх центрів до природних змін у більш короткий термін.

## Перспективне навчання. Недоліки та переваги нових технологій для освіти

Електронне навчання та дистанційні курси дозволяють підвищити кваліфікацію та рівень знань спеціалістів різних сфер діяльності. При цьому на підготовку йде менше часу.

Якщо людина вирішила пройти курси підвищення кваліфікації дистанційно, вона може заощадити бюджет. Також дистанційні курси – це можливість знайти відповідний навчальний заклад не лише у своєму місті, а й по всій Україні чи навіть у світі. Тому курси

та програми навчання більш престижних організацій стають доступнішими.

Тепер кваліфікованим спеціалістам достатньо використати дистанційні технології в освіті. Це дозволить працівникам залишатися затребуваними та підвищити якість трудових функцій.

Процес навчання за допомогою Інтернету розвивається швидко. Проте чи всі викладачі готові змінити звичний спосіб роботи більш просунутий.

Електронне навчання та дистанційні методи подачі матеріалу повинні розвинути потребу у знанні. Але невміле використання сучасних технологій призводить до деформації сприйняття. Повне обмеження живого спілкування, залежність від соціального схвалення та відсутність можливості висловитись – усе це може призвести лише до негативних наслідків такої системи. Якщо електронна освіта не має структури, а пропонується лише як необов'язкове доповнення – якість навчання страждатиме. Важливу роль розвитку електронного навчання грає держава, яка має стимулювати розвиток цифрових технологій.

Переваги нових технологій для освіти:

- навчання у зручному місці;
- стимулювання до самоосвіти;
- швидкий та простий пошук інформації;
- відсутність територіальної прихильності;
- покращення знань щодо способів використання інформаційних технологій;
- доступ до інформації не обмежується літературою навчального закладу тощо.

Інтелектуальний рівень та здатність до самонавчання підвищується при використанні телекомунікаційних технологій. Це сприятливо впливає на освіту людей, допомагає навчитися самодисципліни та правильно шукати інформацію для майбутньої роботи. Електронне навчання та дистанційні курси допомагають старшому викладацькому складу вивчати нові та змінювати звичні способи навчання.

В результаті можна покращити систему навчання, в якій поєднуватимуться практичні навички досвідченого педагога та нова теоретична інформація про напрямок діяльності.

Використання комп’ютера для ознайомлення із матеріалом розвиває абстрактне мислення. Для цього використовуються відеоролики, аудіофайли, презентації та багато іншого.

Оскільки інформаційні технології стають доступнішими, у перспективі їх використання може бути обґрунтовано навіть для дітей дошкільного віку. Наприклад, педагог може використати інтерактивну дошку, відеоролики для наочної демонстрації матеріалів тощо. Дитина зможе швидше освоїтися у цифровому середовищі майбутнього.

**Нові впровадження в сучасну освіту**

*Віртуальна та доповнена реальність.* Візуальні засоби та технології дедалі більше використовуються в освітньому процесі. Справа, знову ж таки, в особливостях нинішнього покоління.

Наші підлітки все роблять за допомогою YouTube – майструють своїми руками, стрижуться та фарбуються, розпаковують посилки та вчать мови. Статистика показує, що YouTube постійно використовують 85% підлітків, при цьому 80% із них стверджують, що відео для них – спосіб дізнатися більше про свої хобі. Не дивно, що викладачі все частіше використовують у навчанні відеоматеріали, фільми та записані лекції.

З розширенням використання сучасних освітніх технологій студенти зможуть вивчати предмети за допомогою технологій віртуальної та доповненої реальності. Наприклад, одягнувши VR-шолом, студент зможе спостерігати історичні події та навіть брати участь у них. Таке навчання називається іммерсивним, воно створює «ефект присутності» і дозволяє переживати неможливий у світі досвід.

Такий захоплюючий сучасний формат навчання дозволить якісніше засвоювати інформацію, адже краще один раз побачити, ніж сто разів почути.

Ми все ще чекаємо, що доповнена реальність штормом пройдеться у нашому світі. На підході Google Glass, Oculus Rift та інші цікаві речі, які принесуть у нашу реальність смак доповненої та віртуальної реальностей.

Очікується, що пристрої, подібні до тих, які ми перерахували, будуть дивувати публіку своїми можливостями, дозволяючи користу-

вачам нашаровувати інформацію на те, що вони бачать, за допомогою контактних лінз або окулярів. В даний час доступ до технологій доповненої реальності в освітніх цілях обмежений переважно програмами для смартфонів.

Наприклад, програма Sky Map дозволяє вивчати нічне небо у пошуках сузір'їв, проте до інтеграції таких програм у школи пройде ще багато часу. Бракує лише цільної системи. Доповнена реальність повинна затягувати та мати підказки для всіх випадків звернення до реальних об'єктів.

За допомогою Google Glass та інших подібних пристроїв, які з'являться у вільному доступі, студенти зможуть досліджувати світ без необхідності відволікатися.

Крім того, відкриваються гігантські можливості для дистанційного навчання. Наприклад, вчитель фізики, Ендрю Ванден Х'ювел зі Швейцарії, транслював те, що відбувається всередині ВАК через Google Glass для своїх учнів за тисячі кілометрів. Вони бачили все так, як він бачив. Функція Hangout тут є особливо корисною для командної співпраці при виконанні проектів та завдань.

В інших випадках студенти можуть бачити додаткову інтерактивну інформацію, наприклад, про історичні артефакти, щоб дізнатися більше про їхню історію. Також може перетворитися реклама, якщо окуляри розпізнаватиме зображення в реальному світі і взаємодіяти з ними.

*3D-принтер.* Юні інженери та їх викладачі – найкращий приклад людей, які потребують 3D-друку під час навчання. У Міннеаполісі одна зі шкіл вже отримала принтер Dimension BST, за допомогою якого учні створюють дизайнерські прототипи.

3D-принтер дозволяє створити робочу міні-модель (і зовсім не обов'язково випилювати її лобзиком із фанери), щоб перевірити інженерну конструкцію, тому студенти можуть відточити свої навички до дрібниць. Сьогодні, володіючи програмами CAD, будь-який студент може заощадити багато часу і грошей, якщо доповнить своє обладнання 3D-принтером.

Не забуватимемо і про те, що 3D-принтери постійно падають у ціні, а значить, незабаром вони стануть доступні всім і кожному. Крім того, фізичні моделі розвивають абстрактне мислення (у всіх у

хімічному класі були наочні молекули?), отже, якщо роздрукувати фізичну версію структури, школярі зможуть краще зрозуміти, з чим мають справу.

*Хмарні обчислення.* Хмарні технології розвиваються, і дуже скоро всі без винятку аспекти нашого життя, у тому числі й освіта, будуть схильні до змін. В аудиторіях майбутнього студентам просто знадобиться електронний пристрій, який надасть доступ до домашньої роботи та інших навчальних ресурсів у хмарі. Жодних важких підручників, всі матеріали будуть доступні доти, доки є з'єднання з Інтернетом.

---

Така зручність надасть студентам певної свободи, адже можна працювати над проектами як удома, так і в будь-якому іншому місці. «Домашня» робота не буде такою домашньою. Цифрова бібліотека буде доступна навіть у відсутності цієї бібліотеки.

Хмарні обчислення прагнуть віртуалізувати класну кімнату. Вищі навчальні заклади можуть використовувати хмарні технології та створювати онлайн-платформи для навчання студентів. Досить просто увійти до системи та відвідувати заняття у віртуальному середовищі.

Візьмемо, наприклад, концепт хмарного віртуального середовища навчання (VLE), яке дозволяє студентам отримати доступ до навчального контенту та брати участь у обговореннях на форумах. Завдання або тести легко можна розповсюджувати по всьому класу, зводячи до мінімуму необхідність бути фізично присутніми студентам, але заохочуючи взаємодію та обговорення; вчителям буде відведено інший канал.

*Соціальні мережі онлайн.* Численні університети вже реєструвалися у віртуальному світі Second Life, щоб надати студентам онлайн-платформу для спілкування один з одним. Будучи великою частиною хмарної платформи, такі соціальні мережі дозволяють студентам зосередитися на навчанні та вільно обговорювати ідеї, тоді як вчителі будуть виступати у ролі модераторів.

Важлива роль у цьому відводиться вчителям, викладачам і професорам, які можуть виступати у ролі керівництва, допомагаючи з відповідями й запитуючи, моментально завантажуючи інформацію у хмарне середовище. Ще одна перевага в тому, що вона є відмінним

інструментом зворотного зв’язку. Соціально-орієнтований підхід у навчанні у майбутньому може стати основою.

*Гнучкі дисплеї.* Ведення конспектів все ще працює, особливо під час лекцій, проте зміщується від паперу до ноутбуків, нетбуків та планшетів. У міру того, як освіта стає більш оцифрованою, можна з упевненістю говорити, що в майбутньому папір відійде на другий план. Як зберегти її зручність?

---

Відповіддю можуть бути гнучкі OLED-дисплеї. Подібні до звичайного паперу, ці дисплеї будуть легкі, гнучкі і неймовірно тонкі. Їх можна буде звернути в трубочку або зберігати чаркою.

На відміну від звичайного паперу ці пластикові електронні документи не тільки довговічні (їх просто не можна порвати), але й інтерактивні. Свайпи, тапи та щипки допоможуть розкрити всі зручності такого паперу.

Ось, наприклад, цифровий папір від Sony, який важить лише 63 грами. Ноутбуки та смартфони не мають такої мобільності.

*Біометрія: відстеження очей.* Ще одна технологія, яка швидко завойовує визнання, – це біометрія. Умовно біометрію зазвичай пов’язують із сферою безпеки, оскільки вона використовує те, що є унікальним для кожного з нас: відбитки пальців, розпізнавання облич, голоси, сітківки ока. З точки зору освіти, установа могла б використовувати відбитки пальців для запобігання прогулам і видачу книг з бібліотеки.

---

Тим не менш, відстеження очей також може бути корисним, наприклад, тим, що надає безцінну інформацію для викладачів. Це ж наочне зображення того, як студент поглинають інформацію та розуміють зміст. У рекламі ці дослідження допомагають визначити, як користувачі реагують на оголошення і що безпосередньо заволодіває їх увагою. Аналогічним чином цю форму аналізу можна використовувати для з’ясування ефективності курсу чи стилю навчання. Mirametrix, наприклад, використовує свій S2 Eye Tracker, щоб оцінити якість навчання студентів за рахунок того, куди вони дивляться під час занять.

Недорогі альтернативи втілюються у формі Eye Tribe для Windows та Android, тому залишається лише питання часу, перш ніж цими даними користуватимуться педагоги.

Дані можуть бути організовані таким чином, щоб кожному з учнів було зручно, тобто відповідно до його стилю навчання. З іншого боку, моделі руху очей також можуть визначати постачання контенту та виявляти проблеми до того, як вони виникнуть. Наприклад, у неправильній подачі матеріалу.

*Мультитач-дисплеї.* За останні кілька десятиліть багато хто побачив появу відеопроекторів у школах, а також перехід від звичайної крейдової дошки до білої дошки. Цілком можливо, наступним кроком буде щось, пов'язане зі смартфонами та планшетами. Наприклад, наступна «дошка» може стати гігантським сенсорним РК-екраном, що дозволяє велику інтерактивність. Основна відмінність між нашими нинішніми сенсорними пристроями та такою дошкою буде в тому, що вона дозволить введення даних одразу від кількох учнів.

І замість традиційної дошки в класі цілком можливо аналог Samsung SUR40 для Microsoft Surface, гігантський планшет у формі столу. Студенти або учні можуть сидіти навколо такого столу-планшета, працювати з вмістом та перетягувати зображення так само просто, як робити нотатки за допомогою віртуальної клавіатури.

## Цікаві приклади використання нових технологій в освіті

*Вчимося граючи.* Сьогодні підлітки, які ростуть у світі, підключеному до Інтернету, страждають на брак концентрації уваги. Це не дивно, оскільки вже з дитинства YouTube, та смартфони завантажують їх оновленнями 24/7, а також надають усі відповіді на запит у «гуглі» або Вікіпедії. Щоб задовольнити покоління, що швидко розвивається, ВУЗам зрештою доведеться відмовитися від традиційних методів зубріння. Зараз важливо не знати масивів інформації, а знати, де її можна дістати – і в цьому є свої плюси та мінуси. Тим не менш, є один спосіб, що дозволяє поєднати приємне з корисним: відеоігри.

KinectEDucation, наприклад, представляє єдину Інтернет-спільноту для зацікавлених педагогів та студентів, які хочуть використовувати Kinect у навчальних цілях. З найкращих прикладів - вивчення мови жестів та гри на гітарі за допомогою апаратного забезпечення від Microsoft.

Інший приклад. Професор із Вашингтонського університету вчить математиці свій клас, використовуючи Kinect, Wii Remote та PlayStation Move. Хороший рівень інтерактивності захоплює студентів та учнів, а інформація тим самим краще засвоюється.

Інший підхід, використовуваний педагогами, спрямований не так на геймплей чи інтерактивність; він наголошує на тому, як студенти можуть навчатися в процесі вивчення створення ігор. Основна ідея в Gamestar Mechanic – навчити студентів базовим навичкам створення ігор (без складнощів програмування), щоб ті могли створити власні ігри, і тим самим навчити їх мові, системному мисленню, вирішенню проблем, написанню сценаріїв, мистецтву та ін.

Студенти навчаються проектуванню, граючи в гру, де вони самі виступають у ролі молодих дизайнерів-початківців, проходячи квести, місії і т. д. заради певних винагород (зон, у яких можна створити власні ігри). Майже нічим не відрізняється від рольових ігор сучасності.

Це показує, наскільки педагоги можуть відійти від традиційного викладання, а студенти – отримувати задоволення від навчання. Цілком можливо, що в недалекому майбутньому діти вважатимуть навчання захоплюючим та захоплюючим. Було б непогано.

*Електронний консьєрж.* Сінгапурський політехнічний університет має «розумний кампус» – коли студенти входять до будівлі, електронний консьєрж автоматично ідентифікує їх. Після цього він може попередити важливі події в університеті або підказати книги, рекомендовані викладачами. Аналіз даних навіть дозволяє виявити студентів, які ризикують не здати вчасно курсову роботу, щоб викладачі могли заздалегідь вжити заходів.

Університет ім. Джон Кертін в Австралії використовує Інтернет речей у своєму університетському містечку. Зі зібраних даних можна робити висновки про зайнятість аудиторій та бібліотек, а також про відвідуваність курсів та повсякденне життя студентів та викладачів. Це допомагає приймати правильні рішення щодо організації навчального процесу.

*Штучний інтелект оцінює якість освіти.* Технологічний університет Малайзії також збирає дані про своїх студентів – з початку і

до кінця їх навчання. Це дозволяє відслідковувати «продуктивність» студентів, що також допомагає університету приймати рішення.

Дослідники констатують, що вже сьогодні штучний інтелект вміє аналізувати проведені уроки та давати поради, як зробити викладання якіснішим, і припускають, що за ШІ майбутнє у системі освіти.

*Віртуальна середня школа.* Учні в Японії можуть відвідувати середню школу, використовуючи гарнітуру віртуальної реальності. За допомогою програми для смартфонів студенти можуть слухати викладачів та проходити тести, а через окрему онлайн-платформу взаємодіяти з іншими школярами.

Учням призначаються вчителі-куратори, які консультують їх з питань навчання та вибору професії, з ними можна спілкуватися телефоном або електронною поштою.

При необхідності можна зустрітися і особисто – в головному кампусі в Окінаві або в кампусах в Токіо та Осаці. Щорічна плата за навчання у цій віртуальній школі становить 100 тисяч ієн ($972). Аналітики вважають, що віртуальна реальність має великі перспективи освіти – до того ж, вона покращує показники успішності.

*Цифрові бібліотеки.* Технологія віддаленого доступу також використовується для підвищення грамотності Камбоджа, де відсутня інфраструктура для поширення книг. У 2015 році в рамках експериментальної програми «Бібліотека в Азії для всіх» було організовано електронні бібліотеки у п’яти початкових школах Камбоджії. Близько 4700 дітей отримали доступ до дитячої літератури у вигляді 100 оцифрованих книг кхмерською та англійською мовами. Щоб це стало можливим, до кожної школи закупили планшети.

**Сучасна освіта в Україні**

Вищого рівня професійної освіти – творчої майстерності – неможливо досягти без загальної гуманітарної освіти і без інноваційних підходів до розв’язання будь-яких проблем (соціально-економічних, виробничо-технологічних, економічних та ін.). Орієнтація на ці стратегічні напрями прийнятна, але консерватизм, властивий вищій школі, перешкоджає рухові вперед.

Головна мета інноваційної освіти – збереження і розвиток творчого потенціалу людини. Проте сьогодні недостатньо творчості та проектування. Освіту потрібно сприйняти як загальнолюдську цінність. Для цього насамперед необхідно зробити так, щоб вона розвивала гармонійне мислення, побудоване на поєднанні внутрішньої свободи особистості та її соціальної відповідальності, а також терпимості до інакомислення.

Сьогодні мисляча людина зобов'язана спостерігати, аналізувати, вносити пропозиції, відповідати за ухвалені рішення й уміти долати конфлікти й суперечності. А для цього вона повинна мати культуру, багатокритерійну установку розв'язання завдань, а також розуміти, що ніхто не може претендувати на істину в останній інстанції і жодну теорію не можна вважати універсальною і вічною.

Освіту можна вважати спрямованою на інтереси особистості, якщо через неї можна розв'язувати такі завдання: гармонізувати стосунки людини з природою через засвоєння сучасної наукової картини світу; стимулювати інтелектуальний розвиток і збагачення мислення, творчість через засвоєння сучасних методів і засобів наукового пізнання; керуючись тим, що людина живе в суспільстві, домогтися її успішної соціалізації через занурення в наявну культуру, зокрема й техногенну, у комп'ютеризоване середовище; враховуючи, що сучасна людина живе в умовах насиченого активного інформаційного середовища, навчити її жити в його потоці, створити умови для безперервної освіти; зважаючи на інтегративні тенденції розвитку науки й техніки та потребу в новому рівні наукової грамотності, створити умови для здобуття широкої базової освіти, яка дасть змогу доволі швидко переходити до суміжних галузей професійної діяльності. Нова освітня парадигма передбачає стосовно вищої освіти також набуття компетентності, ерудиції, формування творчості, культури особистості. У цьому її головна відмінність від старої парадигми, що загалом була спрямована на навчання (її гаслами були: знання, вміння, навички і виховання).

Кроком вперед у сфері освітніх реформ стало прийняття нової редакції закону України «Про вищу освіту». Серед його новацій – фінансова та господарська автономія вишів, можливість обирати адміністрацію, академічна автономія, удосконалення освітнього

держзамовлення, подальший розвиток та імплементація Болонської системи. Фактично українські виші потрапили у конкурентне середовище, в якому роль викладача, його професійність буде вирішальним фактором виживання учбового закладу.

Одним із глобальних досягнень України у сфері освіти, однією з небагатьох державних реформ стало впровадження зовнішнього оцінювання. Корупції у сфері освіти був нанесений нищівний удар, українські абітурієнти по-справжньому отримали рівні права та можливості.

Турбота про якість освіти в країні та її розвиток залежить не тільки від держави, але й від громадянського суспільства, його інститутів, наприклад, таких як Благодійний фонд Октая Алієва. Інновації в освіті вимагають значної акумуляції коштів та ресурсів, а головне – грамотного управлінського підходу, стратегічного планування, контролю та прозорого фінансування.

Інноваційна освіта, що включає в себе новітні методики, максимальну інтеграцію цифрових технологій, – це не далеке завтра, а вже наявна реальність. Будь-яка громадська організація, професійна асоціація чи освітній фонд є сьогодні ключовими елементами в системі сучасної освіти України. Ми відкриті до співробітництва з усіма зацікавленими суб`єктами освітнього процесу в Україні від дошкільного до професійно-технічного та вищого. Сучасна освіта – крок назустріч здоровому, розумному суспільству, Благодійний фонд робитиме усе, аби наша система освіти перейшла на новий рівень.

Система освіти в Україні є однією з важливих конкурентних переваг нашої держави. Саме сучасна освіта формує майбутнє країни, перспективи її розвитку в довгостроковій перспективі. І саме Благодійний фонд Октая Алієва має за мету покращення якості освіти в Україні.

На жаль, сьогодні українські вищі навчальні заклади не спроможні займати високі місця в перших сотнях світових освітніх рейтингів. В оприлюднений список кращих учбових закладів світу за версією британської компанії Quacquarelli Symonds потрапило лише шість українських вишів. Найвищу оцінку отримав Київський національний університет ім. Т. Г Шевченка – 421 місце. При цьому в Україні нараховується 325 вищих учбових закладів  один із найвищих

показників у світі. І, як вважає Благодійний фонд Октая Алієва, саме сучасна освіта може покращити освітній рівень в нашій країні.

Суспільний прогрес, розвиток економічних та політичних інститутів прямо впливають на освітню сферу. Від того, на скільки оперативно система освіти реагує на зміни, залежить її ефективність. Саме задля підвищення швидкості змін Благодійний фонд Октая Алієва запроваджує низку мотивуючих конкурсів та програм.

Сучасна освіта – це відхід від традиційних класичних форм із переходом на платформу інформаційних мереж, зокрема, Інтернет. Сьогодні на порядку денному дистанційна сучасна освіта. Провідні виші світу, такі як Гарвардський університет, Массачусетський технологічний інститут, Стенфордський університет, активно впроваджують форми дистанційної освіти.

На базі цих учбових закладів були розроблені освітні платформи Coursera, EDX, Udacity. Сьогодні через ці освітні системи пройшло більше людей, ніж за всю історію цих поважних учбових закладів. Інноваційна освіта такого формату приречена на успіх і вже починає знаходити шанувальників в Україні. Подібні тенденції прямо впливають на українську систему освіти, обмежуючи її конкурентоздатність.

Сьогодні реформа здійснюється за такими пріоритетними напрямами:

- доступна та якісна дошкільна освіта;
- нова українська школа;
- сучасна професійна освіта;
- якісна вища освіта та розвиток освіти дорослих;
- розвиток науки та інновацій.

Таким чином, ми бачимо, що сучасний період розвитку суспільства характеризується сильним впливом комп’ютерних технологій, які проникають у всі сфери людської діяльності, забезпечують поширення інформаційних потоків у суспільстві, створюючи глобальний інформаційний простір. Невід’ємною і важливішої частиною цих процесів є комп’ютеризація освіти.

# APPLICATION OF TRANSCRANIAL FOCUSED ULTRASOUND IN NEUROSURGERY

**Kosiachuk S. L.,** student of
Kharkiv National University of Radioelectronics
**Storchak O. H. –** Language Supervisor, PhD in Philology, Associate Professor of Foreign Languages Department in
Kharkiv National University of Radioelectronics

**Abstract**. Transcranial focused ultrasound is a modern medical technology that allows a noninvasive neurostimulation on the brain. This technique has been developing for about 20 years and a lot of possible applications of the technology are only at the preclinical research stage. The greatest progress has been made in the field of functional neurosurgery when focused ultrasound allows non-invasive therapy to create small destruction areas in the corresponding targets under constant magnetic resonance imaging (MRI) control to have therapeutic neuromodulatory effects upon Parkinson's disease, essential tremor, pain syndromes, obsessive-compulsive disorders and other diseases. To date, this treatment has been provided for more than 300 patients. The single cases of the ultrasonic thermal destruction of intracranial neoplasms have been published recently. The attempts of ultrasonic third ventriculostomy are made to treat animals.

**Keywords**: neurosurgery, technology, noninvasive neurostimulation, transcranial focused ultrasound.

The **aim** of this research is to review the use of focused ultrasound technology in non-invasive neurosurgery. Ultrasound (US) is the propagation of mechanical energy, elastic waves of mechanical vibration in a medium. Ultrasound can be emitted as continuous waves, which are used for thermal destruction, or intermittent pulses, which have neuromodulatory effects.

The **object** of the research is transcranial focused ultrasound.

The **subject** of the research is the application of focused transcranial ultrasound in non-invasive neurosurgery to have therapeutic neuromodulatory effects.

**The research is of topical interest** as it concerns the treatment of neurodiseases in case it is impossible to apply surgical intervention or when patients face personal contraindications to have invasive treatment. In such cases, modern technologies can provide treatment with ultrasound coupled with MRI for various operations without the use of cranial trepanation. Such an innovative form of non-invasive treatment deals with various non-standard neoplasms as well as with complex forms of nervous system diseases with a chance to be cured.

The **methodology** of the research is based on the modern conception of the technique of the Posttransplant Hemolytic Uremic Syndrome (PHUS) that involves the use of one or more sources focusing ultrasound waves with specific parameters at a given point to produce a desired effect there (e.g. destruction, change in vascular permeability) with constant monitoring of a treatment process by means of ultrasound or MRI. Focused ultrasound surgery (FUS) uses waves with a frequency of less than 1 MHz (the frequency of diagnostic ultrasound is 1-15 MHz) that reduces the heating of cranial bones. Tissue thermal destruction is performed with high intensity ultrasound (>100 $W/cm^{-2}$) whereas non-thermal exposure is achieved with low-intensity ultrasound.

Experiments on the use of ultrasound for the non-invasive treatment of brain substance were first carried out by J. G. Lynn, R. L. Zwemer, A. J. Chick, A. E. Miller in the early 40s of the $20^{th}$ century and continued by the W. J. Fry et al [1; 2].

In the 1950s, ultrasonic destructions were performed to treat Parkinson's disease and mental disorders. Despite the success, several factors – the need for craniotomy, the impossibility of accurate navigation – limited the wide application of the method. These technical problems were solved only in the late 90s of last century. The problem of exposure through skull bones, which significantly attenuate ultrasound and heat up, was solved with the introduction of multiple synchronized ultrasound systems.

Each source has a controller that determines the phase shift so that waves from different sources reach a target simultaneously. The location of sources on the hemisphere evenly distributes heating on the surface of the skull. Accurate navigation has become possible with the advent of MRI and MRT (magnetic resonance thermometry), which provides non-

invasive interactive temperature monitoring during an ultrasonic thermal destruction procedure.

Mechanical energy in ultrasound is transformed into thermal energy due to the friction of particles in a vibrating medium. After a sufficiently intensive or prolonged exposure, coagulation necrosis develops at 56 °C in 1 sec., at 42 °C in 240 sec.

Ultrasound also causes cavitation. In stable cavitation, microbubbles arising in the tissue or introduced from the outside oscillate, resulting in increase in vascular permeability. Unsteady (collapsing) cavitation involves the expansion and subsequent rapid collapse and rupture of micro-bubbles that is accompanied by the release of significant energy and causes mechanical destruction of tissue. Controlled cavitation-assisted destruction is being investigated, but so far this effect is poorly controlled and is primarily seen as a side effect of thermoablation. The parameters of an ultrasonic wave determine the physical effects, which, depending on the location and conditions of application, can have different biological effects.

Nowadays there are more and more possibilities to carry out examinations with different ultrasonic sources. Naturally, good results require equipment of high quality and precision as well as permeability. All modern clinical studies as well as a significant part of the experimental works are performed on a specialized device. In clinical practice, the device is used for non-invasive ultrasound thermal ablation of intracerebral targets.

The device is currently approved during clinical practice in Europe for thalamotomy for essential tremor and neuropathic pain. It has also been demonstrated in a laboratory to be suitable for disruption by cavitation effects as well as for a local increase in the permeability of the blood-brain barrier.

The modern model of the ExAblate Neuro 4000 (InSightec, Haifa, Israel) is a 30 cm diameter helmet containing 1024 ultrasound sources with a frequency of 650 kHz. The source control system allows for a limited focus of ultrasonic waves in the target. An elastic silicone membrane isolates the space between the sources and the patient’s head. Water circulates in this space that prevents the skin and bones of the skull from heating and also acts as a conductor of ultrasound.

The helmet with sources is fixed on a special MRI table which is compatible with General Electric devices having the magnetic field strength of 3 and 1.5 Tesla. It is worth noting that the ExAblate Neuro 4000 and its technology for intracranial targets are currently subject to a number of limitations. In the current model of the device, the zone of possible exposure is limited to an area within about 3.5 cm of the intercommissural line. Exposure to a target outside this zone results in increased bone heating both near the focus and in the vicinity of the cranial vault. A new model has been announced that will have a larger target zone of 6.5 cm in the vicinity of the intercommissural line.

Another issue is the impossibility of achieving the required temperature for thermal destruction in some situations. It is assumed that the limitations can be related to a large volume of the skull above the intercommissural line, the thickness ratio of the compact and cancellous bone of the skull, the shape of the skull and other factors. One way to solve the problem is to introduce microbubbles (ultrasound contrast) into the bloodstream, which can potentiate thermodestruction.

Pre-treatment simulation systems are also being developed that will allow predicting the possibility of thermodestruction even before frame fixation. A feature of the current model is its focus on functional neurosurgery; this results in a small footprint that makes it very difficult to destruct a tumour that can reach a significant size. It has been announced that in a new model of the device the treatment area will be extended to several centimetres.

There are already around 300 patients in the world who benefited from modern technology in the 21st century and there are people whose operations have been carried out using ultrasound. These surgeries must be carried out with the help of sophisticated equipment and highly qualified specialists.

In late 2013 the Rambam Medical Centre in Haifa performed a unique operation using guided ultrasound waves. The operation was performed on the brain under MRI monitoring. Instead of a surgical scalpel, the doctor used ultrasound waves.

A revolutionary breakthrough is that this type of intervention is performed without trepanation of the skull bone and therefore it does not require the use of anesthesia. Since the patient’s skull is not opened, there

is no postoperative rehabilitation period and no danger of postoperative inflammation.

The operation was performed in the neurosurgery department of Rambam Medical Center, using ultrasound waves, on a 72-year-old man from northern Israel, who has been suffering from tremor for almost twenty years. The operation lasted about two hours; after the operation the patient managed to get up and walk on his own. Problems with trembling in hand and body disappeared.

The operation was carried out in such a way that a helmet-like device was placed on the patient's head and the helmet emitted high-powered ultrasound waves which were directed strictly at one area of the brain. The localisation was accurate to within a tenth of a millimeter. During the operation, the patient was positioned inside the tomograph while the operating neurosurgeon sat behind the protective screen. The surgeon activated the helmet device which started emitting ultrasound waves.

The joystick allows the waves to be accurately directed to the area to be burned out that is detected by the real-time MRI scans. The patient was not put under anaesthesia and was fully conscious. During the operation, the neurologist constantly asked questions and monitored the patient's condition, checking his reflexes and ability to function. Just ten minutes after the operation began, one could see a significant improvement in cognitive function: The patient began to control the movements of his own hands.

The surgeries have taken place in America, South Korea, Sweden and Israel. For the first time, doctors have shown that it is possible to successfully perform the most complex brain surgeries without complications accompanying such operations. Other effects are just being introduced into practice.

For example, there are reports of the use of the technique in cancer (thermal destruction of tumours, increase in the permeability of the GEB for chemotherapy). Some techniques have not yet gone beyond research laboratories (cavitation-assisted intracranial target destruction, non-destructive neuromodulation). Some applications of FUS are at an early stage of development and are only potentially being considered for the treatment of CNS pathology. For example, sonodynamic therapy like photodynamic therapy is being considered.

To summarise, ultrasound technique is very promising nowadays and can be developed and refined. Depending on its parameters, PHUS produces several different biological effects that can be used for diagnostic or therapeutic purposes. Some applications of the technology (thermal destruction of targets in the treatment of Parkinson's disease, essential tremor, etc.) are already used in therapeutic practice in clinics in some countries.

They have been adopted as a treatment option. Significant technical, research and clinical work remains to be done on the way to establishing the technique. Nevertheless, it is already possible to state the emergence of a new clinical tool that will complement the existing surgical and radiotherapy methods for the treatment of CNS diseases.

## Reference

1. Lynn J.G., Zwemer R.L., Chick A.J., Miller A.E. A New Method for the Generation and Use of Focused Ultrasound in Experimental Biology // The Journal of general physiology. 1942. Issue 26. P. 179-193.

2. Fry W.J, Mosberg W.H.Jr., Barnard J.W., Fry F.J. Production of focal destructive lesions in the central nervous system with ultrasound // Journal of neurosurgery. 1954. Issue 11. P. 471-478.

# COMPARATIVE ANALYSIS OF WEBSITES TO LEARN FOREIGN LANGUAGE (ENGLISH)

**Lozovyi O.O.,** student of
Kharkiv National University of Radioelectronics
**Storchak O. H. –** Language Supervisor, PhD in Philology,
Associate Professor of Foreign Languages Department in
Kharkiv National University of Radioelectronics

**Abstract**. Nowadays commutation between people around the world is becoming more common but not all the people we communicate with speak the same language we do. That's why there is an international language, English, which people learn in order to communicate with foreigner. Not everybody has enough money to attend classes or hire a private teacher. In this case, there are websites in the Internet to help people learn any language for free.

**Key words**: language, communication, learning, website, Internet.

The **aim** of the research is to get to know how to choose a website to learn English in online education. Online education is a form of education using computers.

A website is a group of web pages connected to each other. Web sites are usually produced by an individual or organization.

The **object** of the research is websites for learning English.

The **subject** of the research is advantages of websites to learn English.

**The research is of topical interest** as we observe an increase in demand of English.

**Research materials** are electronic sources.

The **methods** of the research are analysis, synthesis and comparison.

Websites Bell Labs, The Washington Post, BBC World service, ABC News, and CNN world have been compared by Fedotova O.N. in her paper "Learning English using Internet-resources" [4] using the criterion of informative characteristics. There are more websites on the internet to be compared such as BBC Learning English, Duolingo, Dave's ESL Café etc.

**BBC Learning English**

The BBC Learning English website [1] provides information for learning English for teachers, students and children. The site also provides information about courses, quizzes, vocabulary, pronunciation, news, business etc. Every web page is well structured and informatively given. A multi-language feature is supported for people who are unfamiliar with English. BBC Learning English provides various courses the beginners may need: exam preparation, pronunciation improvement, improving English skills, listening exercises, watching reviews and discussion. The website provides free multimedia and audio files, allowing users to use them for their education purposes and being accessible through different devices. If a user has a question to ask there is a specific section where it can be done. The section is structured to give general information about rules in English, offering a quiz at the end of page where the user is able to ask questions if they have problems with learning English. However, the website is lacking communication with real people that is a problem in learning a foreign language. Communication with native speakers helps a person who improves their spelling, pronunciation and syntax. When studying individually, a human being thinks that when there is a need to communicate with a person, they will face no problem. However, in many cases when a student is communicating they cannot build a sentence correctly, make mistakes in spelling and pronunciation.

In conclusion, BBC Learning English has a lot of webpages which are able to help people enjoy online education and can be used to prepare for exams, review researches and more all over the world. The lack of communication with native speakers has a negative impact on learning English.

**Duolingo**

Duolingo [2] provides listening, audio, reading and grammar exercises. The first thing you can see when opening the home page of the website is nonstandard interface of the website. In order to start free education in learning English, the user has to make an account to proceed. When an account is made, Duolingo website lets the student choose a language the user would like to learn. Once a language is chosen, the website asks if the user has ever studied or spoken the selected language. If

the user has studied the language they select, Duolingo offers three variants of tests to identify their level of English. Each of three tests has different levels of difficulty so that the user can make a choice.

One of the disadvantages of Duolingo is that it confuses the user with its user interface. It can take a minute for the user to get through a web page they want. Because of that, Duolingo shows pop-up messages on screen to help the user navigate the website. The second disadvantage is the lack of multimedia resources BBC Learning English has. Duolingo has speaking exercises where the user has to turn on their microphone to spell a sentence. But if there is no access to the microphone, the exercise can be skipped. Like the BBC Learning English website, Duolingo lacks communication with native speakers. Communication with real people makes learning English better, helps people be more confident.

Duolingo has a system to analyze data. It means that whatever the user has done wrong or right is collected by the website in order to give the user more individual expertize in learning English. If a lot of mistakes are made, Duolingo provides more exercises explaining the rules to help the user understand grammar.

In conclusion, Duolingo is a good website to learn English. However, the lack of multimedia and communication with real people is not a good decision.

**British Council Learn English**

Once the homepage of British Council Learn English [3] is open, the website provides complete information. Art style which is used in the website is minimalistic and it is easy to navigate. The user is able to discover their current English level by taking a free online English test.

In order to start learning English using this website, the user has to register in order to be allowed to choose a kind of education they would like to have. Unlike any other websites that help people learn English, the British Council Learn English website offers three types of online courses: self-study courses, online study courses and personal online tutoring. The website is also offering podcasts, where various topics can be discussed.

A self-study option allows the user to have access to high quality learning material developed by English language experts, from beginners to advanced students. Learning content is added every month, it means that

apart from audio, visual and written learning materials, website releases new content every month to help people improve their English skills.

Live online classes are given by this website at an online conference with a group of students and a teacher. As mentioned before, communication with real people helps to make a student be confident about their speaking, pronunciation and spelling. If there are mistakes, they are better analysed. The user is able to choose time for their online classes.

While on online classes, students can ask teacher various questions about anything that was misunderstood. The website also offers live stream sessions where questions can be asked to improve English skills.

Personal online tutoring is offered as a thirty-minute one-to-one session with British Council. No matter what are the purposes of learning English, an online session with a British Council tutor helps the user meet their needs in learning English.

The user is able to choose any topic or skill they want to improve or it can be selected from a syllabus. The tutor can be asked to give recommendations or advice what is better to learn. Website lets the user to schedule sessions whenever it is comfortable for them including weekends and holidays.

Unfortunately, the British Council Learn English website service is not free, the user has to pay a small amount of money in order to choose the form of education they would prefer. Prices are not as high as big brand English classes have and it is more affordable and flexible.

In conclusion, the British Council Learn English website is comparatively flexible to learn English online. Having online group sessions and personal one-to-one conferences allows people all around the world to communicate in English and improve their skills.

## References

1. https://www.bbc.co.uk/learningenglish/
2. https://www.eslcafe.com/
3. https://www.duolingo.com/
4. Федотова - «Изучение английского языка с помощью Интернет-ресурсов»

# КІБЕРБЕЗПЕКА В АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

**Мельник Б.О.,** ст. гр. М-13-21,
керівник доц. каф. ІПМ Шевченко В.О.
ХНАДУ

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення інформаційно-комунікаційних технологій (ІКТ) та інформаційно-телекомунікаційних систем (ІТС). Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки.

Кібербезпека транспорту – безпека особистих даних, якими користувач ділиться з транспортним пристроєм чи агрегатором транспортних даних. Сьогодні «розумні» системи оточують нас усюди: вони контролюють траси та залізниці за допомогою платформ для моніторингу, відстежують та запобігають заторам як навігатори, відповідають за безпеку пасажирів та водія всередині автомобілів.

Всі ці системи використовують контролери та датчики, які дозволяють тримати зв’язок із зовнішніми джерелами даних. На практиці виявляється, що чим більше у транспортного засобу зв’язку із зовнішнім світом, тим уразливіше для кібератак ззовні він стає і тим більше йому потрібна спеціальна система захисту.

У автомобілебудуванні всерйоз взялися за кібербезпеку і почали інвестувати в проектування та розгортання кіберзахисних рішень приблизно шість років тому. Сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями, але потрібно пройти довгий шлях, перш ніж всі до одного ECU (електронні блоки управління) в машині будуть захищені від кібератак, що зараз активізуються.

Кібербезпека в автомобілебудуванні набагато складніша, ніж на смартфонах та ПК, з двох основних причин:

1. Десятки ECU в кожній машині, з’єднані безліччю електронних шин і відповідають за різні швидкості та характеристики, та

2. Багато потенційних точок доступу, як розташованих всередині автомобіля, так і віддалених, зокрема, OBDII, USB і SD-порти, безключовий доступ, Bluetooth і Wi-Fi, вбудований модем, датчики, інфотейнмент або програми для смартфонів, а також безліч підключень з застосуванням телематики та інших хмарних систем, що мають доступ до систем автомобіля.

У 2015 році дослідники Чарлі Міллер та Кріс Валасек стурбувалися питаннями кібербезпеки та стали досліджувати цю тему на автомобілі марки Jeep. У результаті вони знайшли вразливість у телематичному навігаційному блоці, за допомогою якого дистанційно «залізли» всередину автомобіля та розшифрували повідомлення, які ходили захищеною мережею. Міллер і Валасек змогли віддалено взяти керування автомобілем на себе: почали балуватися вікнами та двірниками, а потім взагалі скинули машину в кювет. Вони могли регулювати швидкість і крутити кермо: це був перший серйозний публічний кейс - після нього автопромисловість почала дивитися на кібербезпеку серйозніше.

Технічно ми можемо уявити собі ситуацію, в якій машина їде швидкісною трасою і їй віддалено вимикають двигун або керування. Чисто теоретично хакер може віддалено перехопити керування у водія, що сидить за кермом. Лякатися, однак, не варто: зробити це вдасться далеко не з кожним автомобілем - все залежить від того, наскільки вразлива електроніка всередині машини.

У 2022 році хакер, який знайшов «ключ» до телематичного блоку, не зможе керувати кермом та гальмами. Раніше блоки всередині автомобіля працювали через центральну шину; зараз вони розділені між собою за функціями і можуть залежати один від одного тільки в їх рамках - без взаємодії з центральною віссю.

Автомобільна кіберзлочинність зростає загрозливими темпами. Наприклад, у Лондоні позаминулого року зловмисники, зробивши дублікат радіобрелка для розблокування іммобілайзера, викрали понад 6000 автомобілів. Кількість викрадень з використанням високотехнологічних засобів збільшується пропорційно до того, як машини «розумніють».

Викрадення машин – вигідний бізнес для всього ланцюжка залучених до неї людей. Саме тому професійні викрадачі мають інструменти і техніку, вартість якої часом досягає декількох мільйонів гривень. З такою допомогою доступно багато чого:

- Клонування електронного ключа – один із найчастіших випадків викрадення. Більшість нових машин обладнано іммобілайзером. Це захисна система, що блокує рух до отримання сигналу від вбудованого в ключ чіпа. Щоб завести автомобіль, потрібно просто зробити дублікат брелока. Робиться це за дві-три хвилини, після чого автомобіль спокійно їде «в нікуди». У зоні ризику — безліч марок і моделей. Ця штатна система захисту потребує додаткового допрацювання;

- Пульт дистанційного відкриття дверей – щастя для автокрадія. Майже всі нові автомобілі продаються із ключами, доповненими кнопками для відкриття та закриття машини. Пульт надсилає не захищений сигнал. За допомогою спеціального приладу – кодграбера цей сигнал уловлюється і у злочинця з'являється можливість спокійно поринути у салон. "Розумні" машини, підключені до смартфону, теж знаходяться у зоні ризику. Власник за допомогою програми на телефоні дистанційно керує деякими функціями автомобіля. Він може запустити двигун, відкрити двері, привести в роботу частину вузлів та агрегатів, контролювати характеристики техніки. Просто так зламати програму смартфона не вдасться, і перехопити сигнал теж. Але якщо заразити телефон вірусом, хакер отримає доступ до управління нарівні з власником.

Найголовніше при виявленні кібератаки - вчасно зупинити її розповсюдження всередині автомобіля. На жаль, більшість сигналізацій не є перешкодою для досвідчених викрадачів. Наприклад, заводський захист, сигналізація з дистанційним відкриттям дверей або з динамічним кодом нічим не краща за штатний пульт. Код перехоплюється тим самим кодграбером, і машина з легкістю відкривається, заводиться і їде.

Та все ж Чарлі Міллер та Кріс Валасек, які зламали Jeep Cherokee, на конференції Black Hat представили недорогий пристрій, який може протистояти атакам хакерів на систему авто. Собівартість такого пристрою становить 150 дол. Воно складається із звичайної

панелі та мікроконтролера NXP. Пристрій підключається до роз'єму під машиною або до приладової панелі (порт OBD2). Пристрій спочатку фіксує характерні параметри автомобіля, але якщо його переключити в режим виявлення, воно виявить аномалії, що відрізняються від стандартної поведінки машини.

Комерційний сектор також розробляє рішення щодо боротьби з кіберзлочинцями: Наприклад, у 2019 році компанія Jaguar Land Rover уклала співпрацю BlackBerry і почала використовувати їхній софт для кібербезпеки у всіх своїх нових автомобілях. За умовами співпраці BlackBerry також допомагає виявляти потенційні вразливості у системах безпеки транспортних засобів, у тому числі у безпілотниках.

Тобто розробки активно ведуться і є певні успіхи. Можливо, найближчими роками всі автомобілі будуть випускатися із системами захисту від хакерського злому. Але що робити власникам сучасних машин зараз?

Купуючи нове авто, необхідно дізнатися, яке електрообладнання і бездротові системи в ньому встановлені. Потрібно знати всі гаджети, що є в машині. При покупці б/у автомобіля обов'язково потрібно заїхати до кваліфікованого електрика, щоб він перевірив весь електроланцюг та виявив наявність додаткового обладнання.

Купувати машину потрібно лише у перевірених автодилерів. Ремонт авто також потрібно здійснювати на перевірених СТО. Горе-ремонтники можуть маніпулювати комп'ютерними системами.

Необхідно захищати важливу інформацію. Якщо в машині встановлена якась система безпеки, то компанія-розробник надає цінну інформацію з управління або розблокування системи та всі необхідні паролі. Ці документи слід зберігати в надійному місці, не можна їх залишати в машині.

Слід бути обережним при покупці автозапчастин та різних пристроїв. Електроприлади, що продаються на ринку, рідко проходять ретельну перевірку або випробування. Якщо встановити такий пристрій, підвищиться вразливість автомобіля.

Бажано знайти кваліфікованого спеціаліста, який стежитиме за оновленням ПЗ або пояснить автовласнику, як це робити.

Слід встановлювати або оновлювати програмне забезпечення лише згідно з рекомендаціями автовиробника.

Важливо приділяти особливу увагу вибору додатків, устаткування чи програм, що вимагають зміна коду ПЗ. Не варто завантажувати неперевірені програми, зокрема музику.

Потрібно не допускати сторонніх осіб та невідомі пристрої до діагностичного порту автомобіля (OBD-II). Зазвичай він розташований з боку водія під панеллю приладів. Через цей порт можна отримати доступ до всіх систем автомобіля.

Не варто передавати смартфони та планшети стороннім особам.

Як би це дивно не звучало, але найефективніші засоби захисту від крадіжки - механічні блокатори. З ними викрадачі намагаються не зв'язуватися. Навіщо витрачати сили та привертати увагу на таке трудомістке завдання, коли можна легко, швидко та безшумно зламати будь-яку електронну оборону.

Кількість автономного транспорту настільки мала, що випадків викрадення повністю без фізичного контакту поки що зафіксовано не було. Але й сучасна техніка перебуває у зоні ризику. Так, змусити її виїхати в сусіднє місто не вдасться, але втрутитися у роботу деяких агрегатів та електронних систем – просто.

Насправді надійно захиститися від атак хакерів на автомобіль можна тільки одним способом - їздити на стареньких «Жигулях», в яких немає електроніки. Такі автомобілі точно ніхто не зламає.

Але ж сучасна людина звикла до комфорту, тому і використовує автомобілі, напхані електронікою. У цьому випадку потрібно дотримуватися вищенаведених порад і при появі надійної системи захисту придбати її та встановити на свій автомобіль. Але варто визнати, що навіть це не гарантує повний захист від хакерського злому.

## Література


1. https://habr.com/ru/company/macloud/blog/564054/
2. https://trends.rbc.ru/trends/industry/614041579a79471ac5adba05
3. https://эксперт-авто43.рф/avtomobilistu/mogut-li-hakery-distantsionno-ugnat-mashinu.html

УДК 536.24

# ПРОГРАМА PVS-STUDIO ДЛЯ ПОШУКУ ПОМИЛОК У ПРОГРАМНОМУ КОДІ НА МОВІ С++

**Біляєва В. А.**
*Харківський національний автомобільно-дорожній університет*

Статический анализ кода это процесс выявления ошибок и недочетов в исходном коде программ. Статический анализ можно рассматривать как автоматизированный процесс обзора кода. Остановимся на обзоре кода чуть подробнее.

Обзор кода (code review) – один из самых старых и надежных методов выявления дефектов. Он заключается в совместном внимательном чтении исходного кода и высказывании рекомендаций по его улучшению. В процессе чтения кода выявляются ошибки или участки кода, которые могут стать ошибочными в будущем. Также считается, что автор кода во время обзора не должен давать объяснений, как работает та или иная часть программы. Алгоритм работы должен быть понятен непосредственно из текста программы и комментариев. Если это условие не выполняется, то код должен быть доработан.

Как правило, обзор кода хорошо работает, так как программисты намного легче замечают ошибки в чужом коде. Более подробно с методикой обзора кода можно познакомиться в книге Стива Макконнелла "Совершенный код" (Steve McConnell, "Code Complete") [1].

Единственный существенный недостаток методологии совместного обзора кода – это крайне высокая цена. Необходимо регулярно собирать нескольких программистов для обзора нового кода или повторного обзора кода после внесения рекомендаций. При этом программисты должны регулярно делать перерывы для отдыха. Если пытаться просматривать сразу большие фрагменты кода, то внимание быстро притупляется и польза от обзора кода быстро сходит на нет.

Получается, что с одной стороны хочется регулярно осуществлять обзор кода, а с другой - это слишком дорого. Компромиссным

решением являются инструменты статического анализа кода. Они без устали обрабатывают исходные тексты программ и выдают программисту рекомендации обратить повышенное внимание на определенные участки кода.

Конечно, программа не заменит полноценного обзора кода, выполняемого коллективом программистов. Однако соотношение польза/цена делает использование статического анализа весьма полезной практикой, применяемой многими компаниями.

Задачи, решаемые программами статического анализа кода можно разделить на 3 категории:

- Выявление ошибок в программах. Подробнее про это будет рассказано ниже.
- Рекомендации по оформлению кода. Некоторые статические анализаторы позволяют проверять, соответствует ли исходный код, принятому в компании стандарту оформления кода. Имеется в виду контроль количества отступов в различных конструкциях, использование пробелов/символов табуляции и так далее.
- Подсчет метрик. Метрика программного обеспечения - это мера, позволяющая получить численное значение некоторого свойства программного обеспечения или его спецификаций. Существует большое количество разнообразных метрик, которые можно подсчитать, используя те ли иные инструменты.

Есть и другие способы использования инструментов статического анализа кода. Например, статический анализ можно использовать как метод контроля и обучения новых сотрудников, еще недостаточно знакомых с правилами программирования в компании.

**Стати́ческий ана́лиз ко́да** (англ. *static code analysis*) - анализ программного обеспечения, производимый (в отличие от динамического анализа) без реального выполнения исследуемых программ. В большинстве случаев анализ производится над какой-либо версией исходного кода, хотя иногда анализу подвергается определенный вид объектного кода, например P-код или код на MSIL. Термин обычно применяют к анализу, производимому специальным программным обеспечением (ПО), тогда как ручной анализ называют «program understanding», «program comprehension» (*пониманием* или *постижением* программы).

В зависимости от используемого инструмента глубина анализа может варьироваться от определения поведения отдельных операторов до анализа, включающего весь имеющийся исходный код. Способы использования полученной в ходе анализа информации также различны - от выявления мест, возможно содержащих ошибки (утилиты типа Lint), до формальных методов, позволяющих математически доказать какие-либо свойства программы (например, соответствие поведения спецификации).

Некоторые люди считают программные метрики и обратное проектирование формами статического анализа. Получение метрик (англ. *software quality objectives*) и статический анализ часто совмещаются, особенно при создании встраиваемых систем.

В последнее время статический анализ всё больше используется в верификации свойств ПО, используемого в компьютерных системах высокой надёжности, особенно критичных для жизни (англ. safety-critical). Также применяется для поиска кода, потенциально содержащего уязвимости (иногда это применение называется *Static Application Security Testing*, SAST).

Статический анализ постоянно применяется для критического ПО в следующих областях:

- ПО для медицинских устройств;
- ПО для атомных станций и систем защиты реактора (Reactor Protection Systems);
- ПО для авиации (в комбинации с динамическим анализом);
- ПО на автомобильном или железнодорожном транспорте.

**Принципы статического анализа**

Большинство компиляторов (например, GNU C Compiler) выводят на экран «предупреждения» (англ. *warnings*) – сообщения о том, что код, будучи синтаксически правильным, скорее всего, содержит ошибку. Например:

```
int x;
int y = x+2;    // Переменная x не инициализирована!
```

Это простейший статический анализ. У компилятора есть много других немаловажных характеристик — в первую очередь скорость работы и качество машинного кода, поэтому компиляторы проверяют

код лишь на очевидные ошибки. Статические анализаторы предназначены для более детального исследования кода.

**Достоинства и недостатки статического анализа**

Главное преимущество статического анализ состоит в возможности существенной снижении стоимости устранения дефектов в программе. Чем раньше ошибка выявлена, тем меньше стоимость ее исправления. Инструменты статического анализа позволяют выявить большое количество ошибок этапа конструирования, что существенно снижает стоимость разработки всего проекта. Например, статический анализатор кода PVS-Studio может запускаться в фоновом режиме сразу после компиляции и в случае нахождения потенциальной ошибки уведомит программиста (см. режим инкрементального анализа).

Другие преимущества статического анализа кода:

1. Полное покрытие кода. Статические анализаторы проверяют даже те фрагменты кода, которые получают управление крайне редко. Такие участки кода, как правило, не удается протестировать другими методами. Это позволяет находить дефекты в обработчиках редких ситуаций, в обработчиках ошибок или в системе логирования.

2. Статический анализ не зависит от используемого компилятора и среды, в которой будет выполняться скомпилированная программа. Это позволяет находить скрытые ошибки, которые могут проявить себя только через несколько лет. Например, это ошибки неопределенного поведения.

Такие ошибки могут проявить себя при смене версии компилятора или при использовании других ключей для оптимизации кода. Другой интересный пример скрытых ошибок приводится в статье "Перезаписывать память - зачем?".

3. Можно легко и быстро обнаруживать опечатки и последствия использования Copy-Paste. Как правило, нахождение этих ошибок другими способами является кране неэффективной тратой времени и усилий. Обидно после часа отладки обнаружить, что ошибка заключается в выражении вида "strcmp(A, A)". Обсуждая типовые ошибки, про такие ляпы, как правило, не вспоминают. Но на практике на их выявление тратится существенное время.

Недостатки статического анализа кода:

1. Статический анализ, как правило, слаб в диагностике утечек памяти и параллельных ошибок. Чтобы выявлять подобные ошибки, фактически необходимо виртуально выполнить часть программы. Это крайне сложно реализовать. Также подобные алгоритмы требуют очень много памяти и процессорного времени. Как правило, статические анализаторы ограничиваются диагностикой простых случаев. Более эффективным способом выявления утечек памяти и параллельных ошибок является использование инструментов динамического анализа.

2. Программа статического анализа предупреждает о подозрительных местах. Это значит, что на самом деле код, может быть совершенно корректен. Это называется ложно-позитивными срабатываниями. Понять, указывает анализатор на ошибку или выдал ложное срабатывание, может только программист. Необходимость просматривать ложные срабатывания отнимает рабочее время и ослабляет внимание к тем участкам кода, где в действительности содержатся ошибки.

Ошибки, обнаруживаемые статическими анализаторами весьма разнообразны. Вот, например, список диагностик, которые реализованы в инструменте PVS-Studio. Некоторые анализаторы специализируются на определенной области или типах дефектов. Другие, поддерживают определенные стандарты кодирование, например MISRA-C:1998, MISRA-C:2004, Sutter-Alexandrescu Rules, Meyers-Klaus Rules и так далее.

Область статического анализа активно развивается, появляются новые диагностические правила и стандарты, некоторые правила устаревают. Поэтому нет смысла пытаться сравнить анализаторы, на основании списков обнаруживаемых дефектов. Единственный способ сравнить инструменты, это проверить с их помощью набор проектов и посчитать найденных ими количество настоящих ошибок.

## Література

1. Макконнелл "Совершенный Код", 2005.
2. https://www.viva64.com/ru/t/0046/.
3. https://www.viva64.com/ru/pvs-studio/ - сайт PVS-Studio.

УДК 536.24

# СТВОРЕННЯ ІГРОВИХ ДОДАТКІВ НА ОБ'ЄКТНО-ОРІЄНТОВАНІЙ МОВІ ПРОГРАМУВАННЯ С ++

**Дяченко Д. С.**
*Харківський національний автомобільно-дорожній університет*

Зміни, що відбуваються сьогодні в різних сферах професійного і суспільного життя, пов'язані перш за все з широким впровадженням засобів інформаційних та комунікаційних технологій. Вони вимагають від фахівця у галузі комп'ютерних наук вміння розробляти програмне забезпечення для розв'язування задач науки, техніки, економіки і управління; створювати і використовувати інформаційні моделі процесів і явищ; використовувати інформаційні технології у науковій, проектно-конструкторській, управлінській та фінансовій діяльності.

Одними з дисциплін, що формують теоретичну і практичну базу у професійній підготовці майбутніх інженерів, є програмування та подібні дисципліни: обчислювальна техніка, інформаційні технології та ін. На сучасному етапі ці дисципліни є невід'ємною частиною вищої освіти. Знання, вміння і навички, отримані студентами в курсі програмування та ін., необхідні студентам при засвоєнні учбового матеріалу більшості дисциплін, передбачених навчальними планами різних спеціальностей [1].

Програмування є однією з фундаментальних дисциплін, що формують теоретичну і практичну базу у професійній підготовці майбутніх спеціалістів ІТ галузей. Крім того, на сучасному етапі програмування є невід'ємною частиною освіти при підготовці математиків, фізиків, хіміків та ін., і тому відповідний курс є складовою навчальних планів цих спеціальностей. Знання, вміння і навички, отримані студентами в курсі програмування, необхідні їм при засвоєнні учбового матеріалу більшості дисциплін, передбачених навчальними планами різних спеціальностей [2].

Програмування – це перша професійно-орієнтована дисципліна, з якою зустрічаються майбутні програмісти під час навчання в

університеті. Від змісту курсу, від методики його навчання, від знань, умінь і навичок, які одержать студенти в цьому курсі, залежить їх подальше навчання, якість засвоєння дисциплін, заснованих на знаннях з програмування, успішність в майбутній професійній діяльності [2]. Тому якість викладання та якість засвоювання цієї дисципліни дуже важливі для майбутніх IT професіоналів.

Однією з провідних IT галузей є розробка та створювання комп'ютерних ігор. Світовий ринок комп'ютерних ігор у 2016 році перевищив позначку у 100 міліардів доларів США, а провідні фірми у цій галузі вже давно мають міліардні статки. Значна частина цих грошей є винагородженням для програмістів. Тому цей, здавалося б, легковажний бізнес насправді дає дуже велику кількість гарно оплачуваних робочих місць для програмістів, у тому числі і в Україні.

Програмування комп'ютерних ігор - це процес створення програмного коду з метою візуалізації ігрового "світу", взаємодії гравця з цим світом і пересування по ньому. Програмування ігор є глибоко командним процесом і підрозділяється на кілька спеціалізованих областей, кожна з яких відповідає за певну функціональну частину майбутньої гри.

Наприклад, провідний програміст займається зведенням всіх підрозділів ігрового движка в єдину працюючу систему, а програміст ігрової механіки - це людина, яка відповідає за програмну реалізацію всіх елементів комп'ютерних ігор. Програміст 3D-движка, програміст графічного движка - це фахівці, що відповідають за відображення ігрового світу на екрані, графічні ефекти і т. п. Програміст мережевого коду відповідає за взаємодію гри і гравця через мережу інтернет (або локальну мережу) з серверами оновлень, іншими гравцями і т.п.

Створення комп'ютерних ігор вимагає спеціальних знань, розуміння того, як працюють ігри та реалізуючи їх програми, великої кількості часу і бажання розробляти вихідний код. Навіть в безкоштовні готові рішення, доступні для використання, вкладені тисячі людино-годин програмування, не кажучи вже про комерційні движки, в які крім часу ще були вкладені і серйозні фінанси.

Значна частина молоді, зокрема, студенти-програмісти є палкими прихильниками комп'ютерних ігор, аж до участі у змаганнях з цих

ігор (від місцевих до світових чемпіонатів). Дехто з них прагнуть самостійно створювати комп'ютерні ігри.

Тому у нашого викладача виникла ідея поєднання вивчення дисципліни "Програмування" при підготовці програміста з розробкою комп'ютерних ігор різного рівня складності (для бажаючих та встигаючих студентів). Цьому сприяло те, що згідно Програми навчальної дисципліни "Програмування" на 2-му курсі вивчається об'єктно-орієнтоване програмування на мові С++, а програмний код більшості комп'ютерних ігор створений на цій мові.

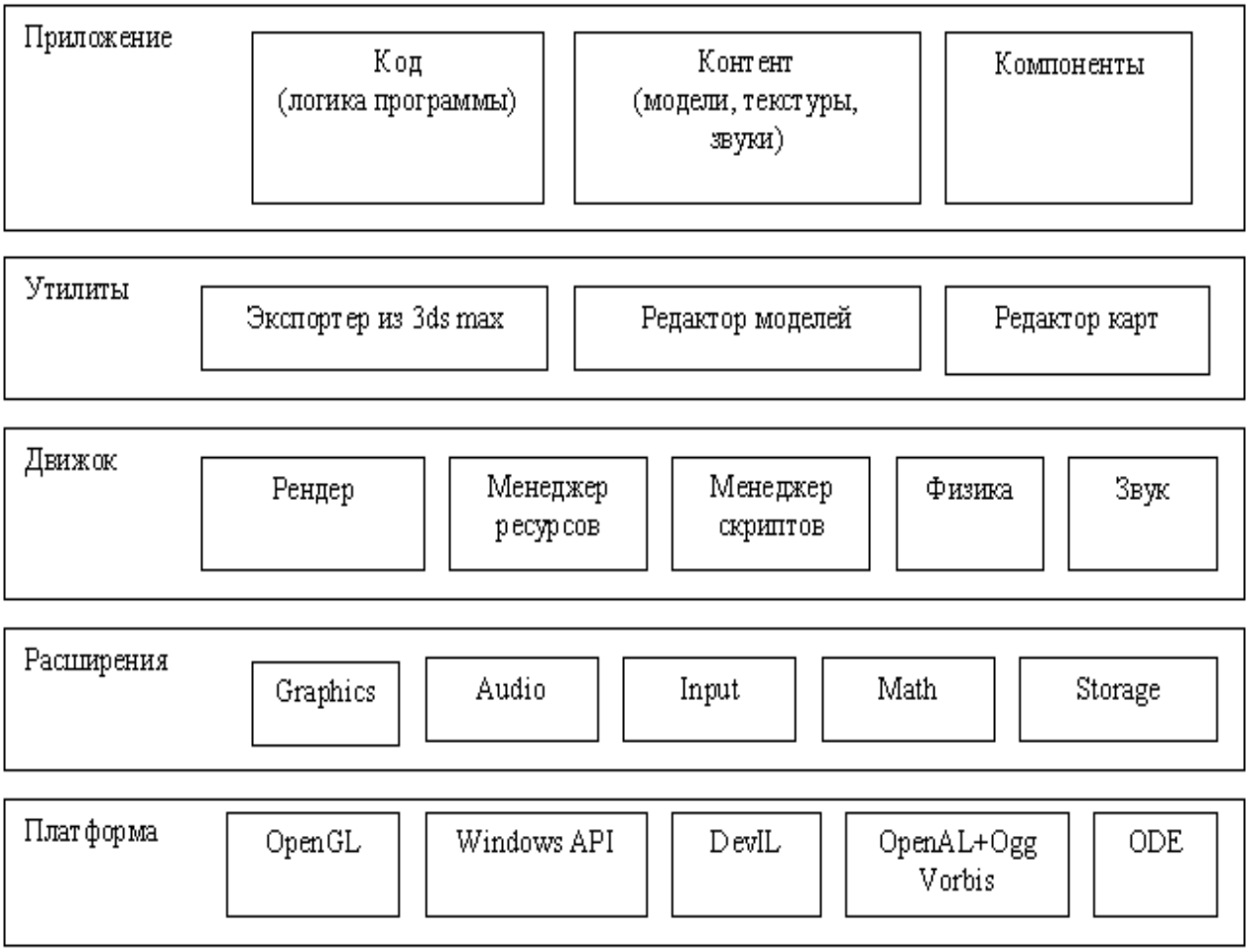


Рис. 1 – Схема створеного програмного проекту

Так як ми використовуємо частину готових бібліотек при розробці ігрових додатків, то деякі низькорівневі конструкції у нас вже є. Наш проект буде виглядати наступним чином (рис.1): на нижньому рівні будуть знаходяться бібліотеки OpenGL, Windows

API, DevIL, OpenAL + Ogg Vorbis, ODE, за ними прошарок з бібліотек і класів нашого движка Engine, який буде містити стандартні для кожного проекту класи і об'єкти, а далі йдуть допоміжні утиліти. На верхньому рівні буде створений додаток з розробленою ігровою логікою.

Наш додаток OpenGL, як і наступні додатки матиме наступну архітектуру: для кожної окремої операції ми будемо використовувати окрему функцію. Більшість з цих функцій будуть викликатися з WinMain, а деякі з MsgProc. У нашому прикладі ми будемо розглядати окремо кожну функцію и її вміст.

Кожна програма Windows повинна мати функцію WinMain. Ми будемо використовувати цю функцію з тією ж метою, що і завжди - як головну функцію програми. Розглянемо вихідний текст нашої функції WinMain:

Перше, що потрібно зробити, це створити головне вікно програми. Ми просто зробили виклик функції InitWindow і створили вікно.

Наступна операція - це ініціалізація пристрою: Init Compatible Context. У цій функції ми зробили попередню ініціалізацію OpenGL. Потім ми провели остаточну ініціалізацію в процедурі InitContext. Контекст в OpenGL – це кореневої об'єкт, який потрібно створити, щоб працювати з OpenGL, в цій функції вже включиться наш відеоприскорювач.

Кожна програма Windows має цикл обробки повідомлень. Обробка повідомлень потрібна для того, щоб відстежувати надходячи в вікно повідомлення від системи - клавіші, згортання і розгортання вікна і т. п.

Ініціалізація OpenGL дуже відрізняється від будь-яких інших комплектів 3d систем і має свою специфіку. Вся система ділиться на OpenGL-специфічні кореневі функції і платформ-специфічні функції. Таким чином, система працює тільки з графікою. Але щоб ініціалізувати OpenGL, необхідно виконати платформ-специфічні функції.

Будь-який додаток OpenGL має виконувати наступну послідовність дій:

**1. Ініціалізація.** На цьому етапі просто підключені всі необхідні динамічні бібліотеки і встановлюються константи. Також при

ініціалізації ми створили основне вікно програми. Ця платформ-специфічна операція, вона не відноситься до OpenGL, а тільки до нашого додатком.

**2. Створення OpenGL контекста.** OpenGL контекст вдає із себе віртуальний об'єкт, до якого прив'язана наш додаток. Таким чином, контекст є, по-перше, кореневих об'єктом OpenGL, і по-друге, сполучною ланкою між нашим додатком і системою OpenGL. В якійсь мірі, контекст OpenGL також є і віртуальним екраном, на якому здійснюється рендер різними функціями OpenGL.

*Створення контексту є платформ-специфічною операцією, функція створення контексту опосередковано вбудована в OpenGL, і для створення контексту існує певна методика.*

***3. Отримання функцій.*** *Сама система OpenGL являє собою набір функцій, але щоб використовувати функції, до них потрібно підключитися. Підключення функцій - це динамічне компонування функцій. У OpenGL недостатньо зробити просто #inlude і потім написати ім'я бібліотеки з функціями. Крім #include, потрібно ще і виконати команду для підключення функцій.*

*У нашій програмі ми використали бібліотеку GLEW, яка також називається як OpenGL Wrangler Library. Таким чином, підключивши бібліотеку GLEW командами #include, ми підключили всі необхідні функції OpenGL.*

**4. Використання функцій.** Після того, як функції були підключені, ми скористалися OpenGL і OpenGL-специфічними функціями. Ці функції мають характерний синтаксис і будь-яку функцію OpenGL можна легко ідентифікувати.

**5. Ініціалізація вікна InitWindow.** Так як ми користуємося функціями Windows, то необхідно на початку програми ввести відповідний #include. Цей рядок підключить необхідні API функції. Усередині функції InitWindow існує два основні виклики - це реєстрація класу вікна.

Зверніть увагу, що при створенні вікна можна вказати різні параметри, в тому числі його розмір.

Тепер здійснимо по порядку всі дії, які потрібні для ініціалізації OpenGL. Операція ініціалізації OpenGL проходить в два кроки. Розберемо перший з них, це операція створення сумісного контексту.

Для цієї операції ми створимо функцію InitCompatibleContext. Ця функція створить контекст таким чином, що контекст створюється на будь-яких пристроях OpenGL.

Установка сумісного OpenGL контексту відбувається в кілька кроків. Перед створенням контексту завжди встановлюється його формат.

Таким чином, функцією SetPixelFormat встановлюється формат кольору пікселів, формат z-буфера, а також інші параметри. Після цього функцією wglCreateContext створюється контекст. Вхідним параметром функції є hDC, тобто дескриптор вікна.

У нашому додатку ми створили вікно попередньо функцією InitWindow, так що інформація про дескрипторі вікна є. Завжди після функції wgl Create Context повинна слідувати функція wglMake Current.

Тепер настав ключовий момент ініціалізації, коли ми повинні прілінковати всі функції OpenGL до нашого додатком. Це робиться дуже просто командою glewInit.

Тепер доступ до функцій OpenGL отримано, і сумісний контекст більше не потрібний, так що ми звільнимо його за допомогою функції wglMakeCurrent с параметром NULL, а також функції wglDelete Context, і перейдемо до наступного розділу, в якому ми створимо основний контекст, тобто такий контекст, який буде працювати з останніми версіями OpenGL.

Спочатку ми створили сумісний контекст OpenGL. Другою дією створили основний контекст. Для цього в нашому додатку є функція InitContext. Можна було продовжувати користуватися сумісним контекстом, але для нашого додатку в цьому немає необхідності. Після створення сумісного контексту, для того щоб отримати доступ до функцій версій OpenGL 4.x був створити основний контекст.

Тепер залишається тільки скомпілювати і запустити додаток. Був розроблений вихідний код цього додатка, і проведена його компіляція.

В операційній системі повинен бути встановлений OpenGL версії не нижче 4.0. У поточних версіях Windows, наприклад Windows 7, а також Windows 8 все вже встановлено, і наш додаток успішно запускається і функціонує на них.

## Література

1. Симбірский Г. Д. Деякі аспекти викладання дисципліни "Програмування" та подібних в транспортних ВНЗ / Г.Д. Симбірский // Інформаційні технології і мехатроніка: міжнар. наук.-практ. конф.: тез. докладів. – Х.: ХНАДУ. - 2016. - С. 126-127.

2. Гришко Л.В. Концептуальні підходи до навчання основ програмування у вищій школі / Л.В. Гришко / Комп'ютерно-орієнтовані системи навчання: Зб. наук. праць / Редкол. – К.: НПУ ім. М.П. Драгоманова. – Випуск 8. – 2004. – С. 134-148.

УДК 536.24

# РИЗИКИ КИБЕРБЕЗПЕКИ ДЛЯ ПІДКЛЮЧЕНИХ ДО МЕРЕЖІ АВТОМОБІЛІВ

**Симбірський Г. Д.**
*Харківський національний університет радіоелектроніки*

Розвиток комунікаційних технологій впливає багато виробничі галузі, зокрема і автомобільну промисловість. На сьогоднішній день, автомобіль обростає все більшим і більшим функціоналом, який покликаний зробити його експлуатацію комфортнішою та безпечнішою для користувача. Такі системи можуть входити до комплектації автомобіля або встановлюються в машину додатково. Але з впровадженням таких технологій, окрім покращення процесу їзди, збільшується і кількість даних, які збираються різними елементами системи підключеного автомобіля, а отже, і кількість персональних даних водія, власника, пасажира, які можуть потрапити не в ті руки та використовуватися не за призначенням.

Перед аналізом питання, які категорії даних збирає підключений автомобіль, розглянемо варіанти підключень автотранспортних засобів:

1. V2V (Vehicle-to-vehicle), бездротова система підключення одного автомобіля до іншого система, головне завдання якої – обмін інформацією між двома автомобілями. З її допомогою, підключений автомобіль може отримувати дані про швидкість руху, місцезнаходження іншого автомобіля. Подібні системи здатні забезпечувати безпеку та контролювати трафік на дорогах.

2. V2G (Vehicle-to-grid), система підключення автомобіля до енергосистем, що дозволяє підключати автомобілі до загальної електричної мережі для підзарядки машини або повернення зайвої електроенергії назад до мережі. Учасники системи V2G зможуть продавати електроенергію в енергосистему – у ті години, коли машина не використовується, і заряджати автомобіль у години, коли електроенергія дешевша.

3. V2P (Vehicle-to-pedestrian) - система взаємодії автомобіля з пішоходами (а точніше їх гаджетами), через яку автомобіль може взаємодіяти з пішоходами, що знаходяться в безпосередній близькості від нього. Отримуючи доступ до частотного діапазону смартфонів, якими користуються пішоходи, сенсори автомобіля можуть дізнатися швидкість та напрямок руху мобільного пристрою, а значить, і пішохода.

4. V2I (Vehicle to Infrastructure), система підключення автомобіля до ресурсів інфраструктури: збирає дані, які виробляє автомобіль та надає інформацію про інфраструктуру водію. Дана система працює в комплексі із системами V2V і так само забезпечує можливість прорахунку найоптимальнішого маршруту та допомагає запобігти можливим ДТП (в автомобілях з автопілотом).

5. V2C (Vehicle to Cloud), технологія підключення автомобіля до хмарних сервісів, що створює канал передачі даних між автомобілем і сервісами збору та зберігання даних, вбудованими в різні програми, які користувач підключає до автомобіля.

Поки що більшість із цих систем підключень присутні в основному тільки в автомобілях, в яких є автопілот, але не виключено, що незабаром вони обов’язково впроваджуватимуться у всі автомобілі та їх екосистеми. І в такому разі в майбутньому при побудові чергового маршруту на сервісі Google Maps ви точно знатимете, що з-за рогу будинку зараз вибіжить людина, і вам слід трохи зменшити швидкість свого автомобіля, щоб не потрапити в ДТП. Але не варто забувати, що з подібним розширенням спектра систем зв’язку зовнішнього світу з автомобілем зростає і рівень загроз злому вашого автомобіля і вилучення з нього ваших персональних даних або приведення в непридатність систем автопілота, що може призвести до ДТП.

Середньостатистичний підключений автомобіль накопичує та обробляє величезний обсяг даних (наведена нижче класифікація даних не обов’язково є повною, а функція збору та обробки тієї чи іншої групи даних залежить від того, які системи та сервіси підключені в автомобілі):

• дані про пересування автомобіля (швидкість, подолана відстань, геолокація автомобіля);

• дані про стан автомобіля (стан двигуна, його температура, тиск у шинах);

• біометричні дані власника авто, водія (наприклад, відбиток пальця, який потрібен для доступу в салон транспортного засобу);

• персональні дані власника автомобіля (його документи, прив'язані до автомобіля, дані про оплату додатків, що використовуються в авто);

• дані зі смартфона, водія, пасажира, зібрані за його підключення до системи автомобіля;

• дані, які отримуються при аудіо/відео фіксації оточення (наприклад, під час використання відео парктроників, установки чорної скриньки в авто).

Існує і окрема група даних, отриманих із підключених автомобілів, класифікована як "Дані, які розкривають кримінальні злочини та інші порушення". Це можуть бути будь-які дані, зібрані автомобілем, і такий статус вони набувають від початку процесу їх використання. Так, наприклад, сукупність даних про швидкість і розташування автомобіля не є даними, пов'язаними з розкриттям злочинів, до початку їх використання в подібних цілях. Така інформація може допомогти поліції викрити водія у порушенні правил дорожнього руху або підтвердити алібі водія, підозрюваного у скоєнні кримінального злочину.

Персональні дані повинні використовуватися з цією метою лише під юрисдикцією уповноваженого державного органу, при цьому не порушуючи права та свободи особи, до якої ці дані належать і відповідно до законодавства держави, в якій потрібне використання цих даних.

Незважаючи на те, що деякі з перерахованих видів інформації безпосередньо можуть і не відносяться до особи водія/пасажира або власника авто, вони все одно можуть відноситись до категорії персональних даних. Найпростіший приклад: за даними, пов'язаними з геолокацією автомобіля, особа, відповідальна за обробку таких даних, може дізнатися про деякі звички та переваги водія/власника автомобіля. Наприклад, часте розташування автомобіля біля храму тієї чи іншої релігійної організації може розкрити приналежність водія до певної релігійної громади, а постійні появи авто біля

закладів відповідної тематики можуть вказати на сексуальну орієнтацію водія/власника автомобіля.

Автомобіль набуває статусу підключеного у разі встановлення в нього спеціального програмного забезпечення (далі ПЗ) пов'язаного з різними системами комунікації та зв'язку. Наприклад, підключеним можна вважати автомобіль, оснащений ADAS (Advanced Driver Assistance Systems – просунуті системи допомоги водієві), які включають:

• радари ближньої та далекої дії;

• зовнішні та внутрішні відеокамери;

• паркувальні радари;

• лазерні далекоміри (LIDAR - Light Identification Detection and Ranging - світлове виявлення та визначення дальності);

• адаптивне керування світлом;

• адаптивний круїз-контроль.

У таких системах збираються дані, пов'язані з пересуваннями автомобіля, та відео фіксацією його оточення. Подібний спосіб отримання інформації пов'язаний із відео/фотозйомкою у громадських місцях. Такі дані відносяться до персональних даних та повинні використовуватися одержувачами та контролерами даних, не порушуючи права та свободи людини, та згідно із законами держави під юрисдикцією якої знаходиться автомобіль.

У 2016 році FIA (The Fédération Internationale de l'Automobile – Інтернаціональна Федерація Автомобілістів) розпочала в Європі кампанію названу "Мій автомобіль – мої дані". Мета - допомогти власникам автомобілів розібратися у своїх правах, пов'язаних із персональними даними. Вони вважають, що для забезпечення прозорості та адекватності збору та обробки даних системами автомобіля потрібно:

• Ввести спеціальні системи оповіщення в автомобілі, які дозволять користувачеві знати, які дані передаються в послуги збору та обробки даних;

• Дозволити власнику автомобіля безпосередньо за допомогою інтерфейсу авто вибирати які дані він хоче передавати до сервісів збору та обробки даних;

• Зобов'язати виробників автомобілів створювати захищені, стандартизовані, мультиплатформні майданчики для можливості

відкритого доступу різних постачальників послуг до даних автомобіля. Існує прецедент, коли використання технологій для підключеного автомобіля стало обов'язковим на законодавчому рівні, а саме ініціатива e-Call. Ця програма була створена в Європейському Союзі, з метою збільшити безпеку користувачів транспортних засобів, дана програма включає сукупність датчиків і ПЗ, покликаних у разі пошкодження автомобіля внаслідок аварії викликати службу 112 передаючи їй координати автомобіля, для якнайшвидшого надання допомоги водію та пасажирам автомобіля . У 2018 ініціатива e-Call стала обов'язково впроваджуватися у всі легкові автомобілі. Існує "Робочий документ про захист даних та впровадження конфіденційності в систему ініціативи e-Call", яким визначаються принципи функціонування e-Call як сервіс, що застосовує збір даних, так само даній ініціативі присвячений розділ у "Посібнику з обробки персональних даних у контексті підключених автомобілів та пов'язаних з ними додатків". З дозволу користувача дана програма може отримувати дані як про автомобіль та ДТП, так і свої особисті дані, наприклад номер страхового поліса, паспортні дані для прискорення процесу надання допомоги, перевірки приналежності до клубів автомобілістів, запобігання проблемам, пов'язаним з мовним бар'єром. Виходячи з положень нормативно-правових актів пов'язаних з даною ініціативою e-Call збирає дані безперервно, але передає їх тільки в момент коли додаток активується, подібний механізм повністю виправданий принципом безпеки персональних даних а саме мінімізації збору та обробки, так як ця програма не виводить дані за межі системи автомобіля до того моменту поки в цьому немає потреби, але той факт, що деякий обсяг даних все одно зберігається в автомобілі створює певні ризики для користувачів.

Через постійне збільшення сенсорів, ПЗ та обладнання в автомобілях збільшується і кількість вразливостей, які можуть спричинити злам автомобіля. Не варто забувати, що машина - це джерело підвищеної небезпеки, і зламування системи навігації в авто, керованому автопілотом, може призвести до дуже сумних наслідків, тому до питань захисту його систем від злому слід ставитися з максимальною серйозністю. Уряд Великобританії випустив керівництво про "Принципи кібербезпеки в підключених та автоматизованих

транспортних засобах". З цього керівництва можна підкреслити 8 основних принципів для створення належного рівня кібербезпеки в системах підключених автомобілів:

1. Питання з організаційної безпеки повинні просуватися на рівні правління компанії;

2. Ризики безпеки повинні оцінюватися та керуватися належним чином;

3. Компаніям необхідно надавати сервісне обслуговування, що включає реагування на інциденти, пов’язані з загрозами безпеці, щоб забезпечити захист систем протягом усього терміну їх служби:

4. Всі компанії, включаючи субпідрядників, постачальників та потенційних третіх осіб, повинні працювати разом для підвищення безпеки системи:

5. Системи захисту повинні бути розроблені з використанням технології багатошарової:

6. Безпека ПЗ повинна бути гарантована на весь термін його експлуатації:

7. Процеси зберігання та передачі даних повинні бути безпечні та мати можливості контролю над ними:

8. Система повинна бути розроблена таким чином, щоб вона була стійкою до атак та реагувала відповідним чином у разі відмови її захисту або датчиків:

Виконання цих принципів виробниками автомобілів, ПЗ та обладнання може гарантувати користувачам безпеку експлуатації систем підключених автомобілів та надійний захист їх персональних даних.

УДК 536.24

# ЗАГРОЗИ КІБЕРБЕЗПЕКИ АВТОТРАНСПОРТНИХ ЗАСОБІВ, ПІДКЛЮЧЕНИХ ДО МЕРЕЖІ ІНТЕРНЕТ

**Симбірський Г. Д.**
*Харківський національний університет радіоелектроніки*

Протягом останніх кількох років набирає популярності концепція connected car – автомобілі з доступом в інтернет. Йдеться не тільки про інфо-мультимедіа системи (музика, карти, фільми на борту доступні на сучасних автомобілях преміум сегмента), а й про ключові як у прямому, так і в переносному сенсі системах автомобіля. За допомогою спеціалізованих мобільних програм можна отримати координати автомобіля, його маршрут, відкрити двері, запустити двигун, включити допоміжні пристрої. З одного боку, це надзвичайно корисні можливості, якими користуються вже мільйони людей, з іншого боку – опинися у викрадача доступ до мобільного пристрою жертви, на якому встановлено таку програму, хіба викрадення авто не стане дрібницею?

У пошуках відповіді на це питання у компанії KasperskyOS вирішили розібратися, що справді може зробити зловмисник, і як власники машин можуть уникнути можливих проблем.

Такі програми зараз популярні: аудиторія додатків найбільш популярних брендів коливається від кількох десятків тисяч до кількох мільйонів користувачів. Нижче для прикладу показано кілька додатків із кількістю їх установок.

Для експериментів було взято кілька додатків для керування різними марками автомобілів. Не розкриватимемо їх назви, але зазначимо, що в ході дослідження компанії розробників про його результати були сповіщені.

Кожна програма була розглянута з наступних позицій:

• чи містить програмний додаток потенційно небезпечні можливості, тобто чи можна за його допомогою викрасти автомобіль або вивести з ладу одну з його систем;

• чи використовували творці програми засоби, що ускладнюють реверс інжиніринг (обфускацію або упаковку). Якщо ні, то зловмиснику не важко прочитати код програми, знайти його вузькі місця і за їх допомогою пробитися до інфраструктури авто;

• чи є програма перевірка на наявність root-прав на пристрої (з подальшою відмовою від установки у разі позитивного результату). Адже якщо шкідливій програмі вдається заразити рутований пристрій, її можливості стають практично безмежними. У цьому випадку важливо зрозуміти, чи використовували творці збереження облікових даних користувача на пристрої у вигляді Plaintext;

• чи є програма перевірка, що після його запуску саме його інтерфейс показується користувачеві (захист від перекриття). Android дозволяє відстежувати який додаток в даний момент показується користувачеві, шкідлива програма може цю подію перехопити - показавши користувачеві вікно фішинга з ідентичним інтерфейсом - і вкрасти, наприклад, облікові дані користувача;

• чи є у додатку контроль цілісності, тобто. чи перевіряє воно себе щодо змін у коді. Від цього залежить, наприклад, чи зможе зловмисник взяти та впровадити свій код у додаток, а потім розмістити його в магазині додатків, зберігши при цьому функціональність та працездатність оригіналу.

Для дослідження було взято сім найбільш популярних програм від відомих брендів і перевірено на предмет слабких місць, якими можуть скористатися зловмисники для доступу до інфраструктури автомобіля.

Аналіз Додатка 1. Механізм реєстрації автомобіля в додатку зводиться до введення логіну та пароля користувача, а також VIN автомобіля. При цьому у додатку є PIN, який треба ввести в систему автомобіля штатними засобами для завершення прив’язки смартфона до машини. Тому лише VIN недостатньо для відкриття дверей авто.

Програма не перевіряє, чи є на пристрої root і при цьому зберігає логін від сервісу у відкритому вигляді у файлі accounts.xml разом з ним і VIN від авто. За наявності у троянця прав суперкористувача на прив’язаному смартфоні ці дані дуже легко вкрасти.

Додаток №1 легко декомпілювати, код можна розібрати. Крім того, воно ніяк не протидіє перекриття власного інтерфейсу, а

значить логін і пароль можна запровадити за допомогою фішингової програми, що складається з 50 рядків коду. Досить перевірити який додаток запущено в даний момент і якщо додаток з цільовим ім’ям пакета, то запустити своє Activity з аналогічним інтерфейсом.

У цьому випадку логін та пароль просто відобразяться на екрані телефону, і нічого не завадить вбудувати надсилання облікових даних на сервер зловмисників.

Відсутність перевірки на цілісність дозволяє будь-кому бажаючому взяти додаток, модифікувати його на свій розсуд і почати роздавати потенційним жертвам. Перевірки підпису не вистачає. Звичайно, така атака вимагатиме від зловмисника певних зусиль – потрібно змусити користувача завантажити модифіковану версію програми. Зате вона носить дуже прихований характер, користувач нічого не помітить, поки його машину не відведуть

З позитивного: програма викликає із собою сертифікати SSL і здійснює з’єднання з їх допомогою. Загалом це запобігає атаці типу Man-in-the-Middle.

Аналіз Додатка 2. Додаток пропонує зберегти облікові дані користувача, але рекомендує зробити шифрування всього пристрою на випадок крадіжки. Розумно, але ми красти телефон не збираємося - ми його "заразили". В результаті та ж загроза, що і в додатку №1 - зберігання логіна разом з паролем у відкритому вигляді у файлі prefs.{??????????}.xml

Таким чином, програма зберегла свою функціональність, але вказані нами при реєстрації логін і пароль були виведені на екран смартфона відразу після спроби входу в систему.

Аналіз Додатка 3. Автомобілі, що використовують цю програму, за бажанням замовника комплектуються модулем керування, який може запустити двигун та відкрити двері. Його встановлює дилер, при цьому кожен модуль комплектується стікером з кодом доступу, який видається на руки власнику машини. Тому прив’язати автомобіль, знаючи його VIN, до чужих облікових даних не вдасться.

Однак є інші можливості для атаки: по-перше, додаток дуже маленький, всього 180 кілобайт в APK-виді, по-друге, вся програма обкладена налагоджувальною печаткою в лог-файл, який зберігається на SD карту.

Аналіз Додатка 4. Додаток дозволяє підчепити існуючий VIN до будь-яких облікових даних, але сервіс обов'язково надійшле запит на бортовий комп'ютер автомобіля. Тому найпростіший крадіжка VIN не допоможе розкрити машину.

Проте досліджуваний додаток беззахисно перед перекриттям свого вікна, і якщо завдяки цьому у зловмисника виявляться логін та пароль від системи, він зможе відкрити авто.

Аналіз Додатка 5. Щоб прив'язати автомобіль до смартфона, на якому встановлено цю програму, потрібен PIN-код, який повідомить бортовий комп'ютер авто. Отже, як і у випадку з попереднім додатком, одного VIN недостатньо, потрібен доступ до автомобіля.

Додаток від російських розробників, який концептуально відрізняється від своїх аналогів тим, що в якості авторизації використовується номер телефону власника.

Такий підхід створює неабиякий ризик для власника автомобіля: для початку атаки потрібно виконати одну API функцію Android та отримати в результаті логін до системи.

Аналіз Додатка 6. З особливостей останнього розглянутого додатка варто відзначити зберігання логіну та пароля у відкритому вигляді у файлі credentials.xml.

Успішне зараження смартфона троянцем з правами суперкористувача дозволить без особливих зусиль вкрасти цей файл.

Теоретично, після крадіжки облікових даних зловмисник зможе отримати контроль над автомобілем, проте це не означає, що злочинець зможе просто його викрасти. Справа в тому, що для того, щоб рушити на авто обов'язково наявність ключа, тому, потрапивши всередину машини, викрадачі використовують блок програмування і записують в борт управління авто новий ключ. А тепер згадаємо, що майже всі описані програми дозволяють розблокувати двері, тобто. зняти машину із охоронної сигналізації. Таким чином зловмисник проробить всі необхідні для угону операції потай і швидко, не треба нічого ламати або свердлити.

Також не слід обмежувати ризики власника одним лише викраденням. Отримавши доступ до авто, його можна зіпсувати так, що жертва потрапить в аварію і може зазнати серйозних травм або загинути.

Жоден із розглянутих додатків немає повного захисту. Однак треба віддати належне розробникам додатків та сервісів – дуже добре, що для керування авто у жодному з описаних випадків не було використано голосових або SMS каналів. Однак саме такими засобами користуються виробники охоронних сигналізацій. З одного боку, нічого дивного в цьому немає, якість мобільного інтернету не завжди і не скрізь дозволяє авто бути онлайн, у той час як голосові дзвінки та SMS як базові функції будуть доступні. З іншого боку, це створює додаткові загрози безпеці авто, розглянемо які саме.

Голосове управління відбувається з допомогою про DTMF команд. Власнику потрібно в прямому значенні слова зателефонувати автомобілю, охоронна сигналізація відповість на вхідний дзвінок і приємним жіночим голосом повідомить статус автомобіля, після чого перейде в режим очікування команди від власника. Для того щоб змусити авто відкрити двері або запустити двигун, достатньо буде набрати відповідні цифри на клавіатурі телефону. Сигналізація розпізнає коди та виконає потрібну команду.

Творці таких систем подбали про безпеку та передбачили список дозволених номерів, яким дозволено керувати автомобілем. Проте, ніхто не подумав про ситуацію, коли телефон власника скомпрометований. Тобто зловмиснику достатньо заразити телефон жертви примітивним додатком, який від її імені дзвонитиме охоронної сигналізації. Якщо при цьому вимкнути звук динаміка та екран, можна керувати автомобілем повністю непомітно для жертви.

Звичайно, не все так просто. Наприклад, багато автолюбителів зберігають номер охоронної системи під вигаданим ім’ям, тобто. для успішної атаки необхідно, щоб жертва часто взаємодіяла з авто через дзвінки. Тільки так зловмисник, який викрав історію вихідних дзвінків, може знайти номер авто у списку контактів жертви.

Творці іншого методу управління охороною автомобіля - за допомогою SMS-команд - точно не читали жоден з наших оглядів з безпеки пристроїв на базі платформи Android. Справа в тому, що першими та найчисленнішими мобільними троянцями, з якими боролася компанія, були SMS-троянці. Тобто зловреди, що містять у своєму коді можливість прихованого надсилання SMS; причому таке відправлення здійснювалося як у ході штатної роботи троянця, так і

по віддаленій команді зловмисників. В результаті, для того, щоб відкрити двері авто жертви, господарям зловреда достатньо виконати три дії:

1. Перебрати SMS на смартфоні на предмет команд автомобілю.

2. У разі виявлення потрібних SMS, витягніть з них номер телефону та пароль доступу.

3. Надіслати на виявлений номер SMS із текстом, що відкриває двері авто.

Усі три операції троянець може зробити потай від жертви, єдина складність, з якою, утім, зловмисники вміють справлятися, — це зараження смартфона.

Автомобіль — річ дорога, і до безпеки потрібно підходити не менш ретельно, ніж до безпеки банківського рахунку. Зрозуміло, зрозуміла позиція автовиробників і розробників, які намагаються оперативно випускати на ринок програми з новими можливостями для зручності власників машин. Однак думаючи про безпеку connected car не варто обмежуватися безпекою інфраструктури (серверів управління), каналами взаємодії авто та інфраструктури. Варто також звернути увагу на бік клієнта, зокрема на програму, яка зараз знаходиться у користувачів. Зараз його дуже просто обернути проти його власника, і це, можливо, зараз найвужче місце, на яке можуть націлитися зловмисники.

Тут слід сказати, що поки ми не бачили жодного випадку атак на програми для керування авто, жоден з тисяч виявлених нами нових зловредів поки не містив код для завантаження файлів конфігурації таких додатків. Однак сучасні троянці дуже гнучкі, якщо сьогодні один такий троянець показує персистентну рекламу (яку користувач сам ніколи не зможе видалити), то завтра він за командою зловмисників завантажить на C&C конфігураційний файл автододатку. Або видалить його та поставить поверх інше – модифіковане. Як тільки це стане фінансово вигідно зловмисникам, нові можливості для звичайних мобільних троянців не забаряться.

## Література

1. Https://securelist.ru/mobile-apps-and-stealing-a-connected-car/30188/.

# МАТЕРІАЛИ
# 84-ої МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ ХНАДУ

Відповідальний за випуск *Г.А. Плехова*

В авторській редакції