ТЕНДЕНЦІЇ РОЗВИТКУ ІТ-ТЕХНОЛОГІЙ В УКРАЇНІ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ
БІЗНЕС-КОЛЕДЖ
засновано в 1966 році

МАТЕРІАЛИ

XIII Всеукраїнської

студентської науково-практичної конференції

студентів, аспірантів та молодих вчених

за тематикою
«Тенденції розвитку
ІТ-технологій в Україні»

22-23 квітня 2021 р.
м. Черкаси

Міністерство освіти і науки України

Черкаський державний бізнес-коледж

МАТЕРІАЛИ

XIII Всеукраїнської

студентської науково-практичної конференції

студентів, аспірантів та молодих вчених

за тематикою

«Тенденції розвитку ІТ-технологій в Україні»

22-23 квітня 2021 р.
м. Черкаси

УДК 004.7+00.5

Матеріали XIII Всеукраїнської студентської науково-практичної конференції студентів, аспірантів та молодих вчених за тематикою «Тенденції розвитку ІТ-технологій в Україні»: збірка наукових праць. Черкаси, 2021, 204 с.

ISBN 777-777-7777-77-7 (електронне видання)

Доповіді наукової конференції містять результати досліджень за наступними напрямками: перспективи розвитку чат-ботів в сучасному світі, виклики робототехніки в сьогоденні, розвиток сучасних проблемно-орієнтованих додатків, сучасні напрямки розвитку веб-технологій, кібернетична безпека.

Роботи друкуються в авторській редакції. В збірці максимально зменшено втручання в обсяг та структуру відібраних до друку матеріалів. Редакційна колегія не несе відповідальності за достовірність досліджень, матеріалів та результатів досліджень, що надано в рукописах, та залишає за собою право не розподіляти погляди деяких авторів на ті чи інші питання, висвітлені в роботах.

Збірник становить інтерес для студентів, аспірантів, викладачів та наукових працівників.

УДК 004.7+00.5

ISBN 777-777-7777-77-7

ЗМІСТ

Секція 1.

Перспективи розвитку чат-ботів в сучасному світі

Створення чат-ботів в Україні

Гетьман Денис Ігорович
Черкаський державний бізнес-коледж
Науковий керівник:
Підласий Андрій Іванович

Питання застосування систем віртуального спілкування на основі штучного інтелекту досліджують на протязі багатьох років. На сьогоднішній день проблема віртуального спілкування актуальна через швидкий доступ до інформації, можливості одночасної роботи в системі багатьох користувачів, обміну інформацією, взаємодії з метою вирішення будь-яких питань, підтримки навчання, комунікації з клієнтами і партнерами по бізнесу, проведення аналітичних досліджень, збору необхідної інформації, підвищення кваліфікації та інших переваг.

Основними питаннями в створення систем спілкування є розробка моделі спілкування, моделі учасника спілкування, розвиток засобів, в першу чергу, семантичних і прагматичних, опису навколишнього середовища (моделі мови, моделі користувача, моделі навколишнього середовища, моделі системи спілкування). Тому для вирішення цих питань необхідно визначення принципів роботи, особливостей імітації мовної поведінки людини в процесі спілкування, розробка моделі спілкування, написання чат-бота.

Серед програм-співрозмовників є програми, створені на основі штучного інтелекту - чат-ботів.

Чат бот - це комп'ютерна програма, що імітує інтелектуальні бесіди з людьми, зазвичай через аудіо або текст. Мета полягає в тому, щоб замість простого пошуку інформації на вашому сайті клієнт міг взаємодіяти з чат ботом, щоб знайти те, що йому потрібно.

Чат боти зазвичай використовуються для відповіді на прості запитання, включаючи основну інформацію про продукти, прогнози погоди або інформацію про компанію. Однак в деяких додатках бесіди чат ботів можуть поєднуватися з реальними людьми для відповіді на питання, які є більш складними.

Серед достоїнств чат бота - його здатність до навчання. Він може вчитися з попередніх розмов, стаючи все більш і більш ефективним. Чим більше знань він отримає, тим краще він зможе відповідати на запити майбутніх клієнтів.

Наша країна впевненно йде вперед в IT-індустрії. З збільшенням популярності чат-ботів спеціалісти IT-компаній отримують все більше замовлень від замовників щодо створення для них такого боту. Потребуються в такому вони , тому що боти срощують нам життя та облегчують більшість задач. Особливо це позначається на людях , що мають свій онлайн - бізнес.

Що може робити бот на прикладі створення його для свого бізнесу:

1. Автоматизацію процесу продажів

Чат бот може продавати Ваші продукти або послуги 24/7, він фактично заробляє вам гроші, поки ви спите.

Чат - бот, який оперативно приймає замовлення, покращуючи Ваше взаємодія з клієнтами та заощаджує Ваш час, не відволікаючи від виконання різних підприємницьких завдань.

2. Обробку платежів

Чат бот може успішно приймати і обробляти платежі. Використовуйте чат бот як платіжний інструмент, якщо клієнту необхідно внести платіж. Чат - бот може без зусиль обробити транзакцію.

Ви спрощуєте своєму покупцеві процедуру оплати. Всього за пару кліків ваш клієнт отримує можливість оплачувати товари або послуги через месенджер на своєму смартфоні.

3. Аналіз клієнтської бази

Однією з найпотужніших можливостей чат бота є здатність збирати інформацію про ваших клієнтів. За допомогою цієї інформації ви будете краще підготовлені до більш ефективного маркетингу для своїх клієнтів в майбутньому.

Ви можете дізнатися, які продукти або послуги вони вважають за краще (і, в свою чергу, повідомити їм, які типи продуктів є на складі), а також використовувати

цю інформацію для своєї тематичної стратегії, оптимізувавши його під запити вашої цільової аудиторії.

У цій роботі був проведений аналіз особливостей імітації мовної поведінки людини в процесі спілкування, визначено основні функції та принципи роботи чат-бота з метою розробки моделі спілкування.

Унікальні можливості Інтернету такі, як швидкість, оперативність, доступність комунікації між користувачами - дозволяють використовувати мережу як засіб спілкування і створювати інтерактивні форми спілкування. На зміну реальним співрозмовникам приходять програми штучного інтелекту. Але, на відміну від розмови людей, програма не володіє гнучким розумовим інтелектом. На жаль, сучасні віртуальні співрозмовники лише частково вирішують питання імітації розмови людини. Словниковий запас більшості віртуальних співрозмовників обмежений, крім цього, у них відсутня емоційне забарвлення, тембр голосу тощо., Тому більшість віртуальних співрозмовників запрограмовані на ведення нескладної бесіди.

Література

1) Telegram Bot API [Електронний ресурс] : Telegram Documents.

2) Аванесян Н. Л., Telegram, как пример мессенджера: возможности и перспективы развития. [Електронний ресурс] / Н. Л. Аванесян // Научный потенциал XXI века. – 2017.

3) Агальцов, В. Базы данных: В 2-х книгах. Книга 2: Распределенные и удаленные базы данных : Учебник / В. Агальцов – Москва : Форум, 2018. – 271 с.

4) Архаков, Д. NodeJS: Делаем кнопки в Telegram API (inlinekeyboards) [Електронний ресурс] / Д. Архаков // Блог о программировании. – 2016.

ВИКОРИСТАННЯ ЧАТ-БОТУ ДЛЯ ПОКРАЩЕННЯ НАВЧАЛЬНОГО ПРОЦЕСУ В ЗАКЛАДАХ ОСВІТИ

Копачев В. С.
КНУТД
Науковий керівник: Хотунов В. І.

З кожним роком популярність чат ботів зростає. Адже на сьогодні кожен має можливість за допомогою них налаштувати зручний інтерфейс зі своєю програмою або сервісом. Сфер застосування ботів безліч. Однією з таких є використання чат-боту [1] для покращення навчального процесу.

Зараз в закладах освіти є сайти [2] для налагодження навчального процесу. На таких сайтах можна знайти актуальну інформацію про розклад занять, дзвінків, їх заміни та інформацію про викладачів. На основі цієї інформації є можливість сформулювати функціонал для покращення навчального процесу. До такого функціоналу можна віднести наступні пункти:

- пошук занять на сьогодні;
- перегляд розкладу дзвінків;
- перегляд поточного навчального тижня;
- перегляд замін у розкладі;
- перегляд розкладу для викладачів;
- перегляд повних імен викладачів;
- пошук викладача за його розкладом;
- пошук вільного кабінету для проведення заняття.

Використовуючи чат-бот в якості інтерфейсу для переліченого функціоналу з’являється можливість запам’ятати групу і підгрупу студента, щоб надалі показувати персональний розклад. Використання розпізнавання команд з контексту повідомлень робить взаємодію з чат-ботом інтуїтивно зрозумілою. Також з’являється інструмент для інформування студентів окремої групи чи відділення, при нагоді поширити нагальні події, новини чи зміни.

Підбиваючи підсумки чат-бот це чудовий засіб для покращення начального процесу, який стане у нагоді як студентам, так і викладачам, для доступу до якого необхідний лише інтернет та додаток у мобільному чи вебсайт.

Література:

1. CSBC Bot [Електронний ресурс] – Режим доступу до ресурсу: https://t.me/chsbc_bot

2. Moodle [Електронний ресурс] – Режим доступу до ресурсу: http://78.137.2.119:1919/m72/

ДОРЕЧНІСТЬ ЗАСТОСУВАННЯ ЧАТ-БОТІВ У РОЗРОБЦІ СУЧАСНИХ ОНЛАЙН-СИСТЕМ

Красноштан Д. В.
Черкаський державний бізнес-коледж
Підласий А. І.

Сучасні онлайн-системи стали набагато складніші, ніж просто сайт чи енциклопедія. До того ж, інформація стає індивідуальною та «рекомендованою» особисто, наприклад, здійснивши однаковий пошуковий запит з різних пристроїв та, тим паче з різних облікових записів, можна отримати певну різницю в результатах. Орієнтація на користувача стає все дужче помітною. Це суттєво ускладнює навіть прості сайти в інтернеті, оскільки потребує ретельного налаштування, адміністрування та аналізу [1].

Тим не менше, розробка навіть простого сайту на купленому сервері (здебільшого купуються використані ресурси – трафік, вільне місце чи потужність) вже є досить незвичайною задачею та потребує уважного розгляду, оптимізації ресурсів, просування тощо. Такими речами займаються окремі спеціалісти – DevOps [2]. Звісно, існує багато готових сервісів, що надають можливості з безкоштовного створення сайтів. Проте, якщо розглядати сайт із точки зору подальшого розвитку (хоч і невеликого), то не всі можливості, особливо прості та незначні, можуть бути доступні до реалізації. Наведемо приклад: припустимо ви хочете зробити власний

блог із просунутими можливостями коментування. Можна створити «сплав» блогу із форумом, проте затрати на таку реалізацію будуть суттєвими, а масштабованість можливостей та організація спілкування може бути не надто високою. Необхідне якесь більш універсальне рішення.

Плавно ми підійшли до такого поняття, як чат-боти. Бота можна розглядати як і просту програму, що обробляє й видає який-небудь текст, так і віртуальних співрозмовників і консультантів [3]. Варто приділити особливу увагу ботам, що можуть бути вбудовані у месенджери, бо такого роду програми є практично на усіх користувацьких пристроях – навіть на смарт-годинниках. А це значить, що за доречної й відповідної імплементації ви можете отримати дуже велику кінцеву авдиторію.

Основні та найбільш популярні месенджери, що підтримують ботів, це Viber, Telegram та Facebook Messenger. Однозначно, найбільш потужні рішення надає платформа Telegram. З недавнього часу напрочуд швидко розвинулися можливості у чатах та групах: можна закріплювати купу повідомлень, спілкуватися не лише через текстові чи аудіоповідомлення, а ще й голосовим чатом – щось посереднє між груповим дзвінком та класичними аудіоповідомленнями [4]. Всі ці групові можливості можна вдало підкріпити керуванням та обробкою з боку ботів, що можуть виконувати гнучкі ролі прямо усередині цікавого групового обговорення…

Інші месенджери більш сфокусовані та надають лише основні можливості для ботів, як-от прийом та відправлення медіа та текстових повідомлень тощо. Ботів можна розглядати і як спосіб швидко отримати певну інформацію від користувачів й навпаки, так і спосіб нагадати співрозмовникові про якусь певну подію. Ці можливості можуть креативно переплітатися між собою та розвивати небачені досі грані спілкування (особливо групового), перетворюючи звичний підхід до інформації у зручний та налагоджений «придаток» реального життя й спілкування.

Якщо ж вас цікавлять фінансові сторони даного питання, то варто обговорити кілька часто використовуваних моделей та відповідні особливості:

- класична реалізація на сервері, можливо орендованому (потребує детальних знань, ціна може бути значно вище за створення сайту);
- безкоштовна реалізація через іншого бота, «посередника» (керуючий бот повністю покладає на себе питання зі створення та обслуговування вашого бота, але може іноді «вимикатися», можливий показ рекламних оголошень/повідомлень тощо);
- платна реалізація через стороннього бота-посередника (дуже вдалий варіант, що схожий на попередній, проте ще й із покращеною стабільністю, отож ви маєте змогу фокусуватися вже на розробці функціоналу, а не на процесах «початкового будівництва»).

Можете лише уявити, які можливості надасть вашому проєкту вдале та доречне використання ботів: суттєво полегшиться обмін інформацією із користувачами, зменшиться навантаження на основну онлайн-систему, майже кожна людина може дуже просто, ефективно та швидко передати інформацію, спроститься управління групами та чатами… Більш того, використання трафіку при спілкуванні із ботом через месенджери вкрай мале, оскільки передаються крихітні шматочки інформації. Отож, охоплення клієнтів вашого проєкту буде ще більшим навіть у регіонах із не дуже швидким інтернетом.

Підсумовуючи вищевикладене, ми дійшли таких висновків: за вдалої реалізації боти у месенджерах стануть доречним доповненням до класичного сайту чи сторінки у соцмережах; можна поєднувати елементи передачі інформації з інтеграцією ботів до груп чи чатів, таким чином створюються досі небачені можливості ефективного спілкування та командної роботи; наявність месенджерів для різних апаратних і програмних платформ дозволяє виходити на контакт навіть тоді, коли користувач не знаходиться безпосередньо за ПК тощо. Однозначно, бот не може повністю замінити потужний сайт, але для стартапів він може бути напрочуд гарним рішенням, у тому числі й як доречне доповнення основного функціоналу вже для більш складних проєктів.

Література:

1. Что такое AWS – AWS. URL: https://aws.amazon.com/ru/what-is-aws/
2. DOU – Карьера в IT: должность DevOps engineer. URL: https://dou.ua/lenta/articles/devops-engineer-position/
3. Чат боты для сайта – Чат боты: примеры использования и перспективы развития. URL: https://bot.konveier.com/2019/07/20/chat-boty-primery-ispolzovaniya-i-perspektivy-razvitiya/
4. Голосові чати 2.0: канали, мільйони слухачів, записування, інструменти для організаторів – Блог Telegram. URL: https://telegram.org/blog/voice-chats-on-steroids/uk

УДК 314.743

ЧАТ-БОТИ – НОВА ОСНОВА СФЕРИ ПІДТРИМКИ ТА МАЙСТРИ ЗАОЩАДЖЕННЯ

Пономарьов Д.Е.
dmitroponomarov9@gmail.com
Черкаський державний бізнес-коледж
Оліфіренко В.М.
м. Черкаси, Україна

Чат-ботом зазвичай називають програму на основі штучного інтелекту. Вона імітує інтерактивне спілкування з людиною основуючись на фразах користувача та заздалегідь розрахованих текстових або слухових сигналах.

Ринок чат-ботів невпинно росте логічних на те причин:

- ✓ боти вміють закривати прості повідомлення (віртуальний помічник пише першим та пропонує варіанти відповіді, здатний відповідати на прості питання а інші передає оператору);
- ✓ дані програми здатні цілодобово збирати та кваліфікувати так званих лідів (у цьому випадку бот сам питає, що клієнт бажає купити і на основі цих даних збирає контакти, потім передає дані оператору, який вийде на зв'язок з покупцем в робочий час);

- ✓ видавати цілий спектр потрібних покупцеві товарів та продуктів; розповідати користувачам про оновлення та здійснювати з ними зворотній зв'язок.

Згідно з дослідженням Business Insider, ринок чат-ботів чекає зміна сукупного середньорічного темпу зростання, CAGR, на 29,7% з 2,6 млрд доларів в 2019 році до 9,4 млрд доларів до 2024 року. Згідно досліджень компанії Oracle чат-боти можуть заощадити приблизно 174 мільярдів доларів у напрямах з фінансових питань, продаж, страхування та підтримки клієнтів.

Та по при всі свої переваги чи зможуть боти остаточно замінити живих співробітників служби підтримки або іншого підрозділу завданням якого є спілкування з клієнтами? Зазвичай чат-боти є помічниками для людей. Але вони не можуть виконувати складних завдань, оскільки сам їх процес мислення обмежений тим що прописано в програмному коді. Продовжуючи цю тему варто зазначити цікавий факт. У 2020-му році компанії Facebook та Pandorabots провели першу зустріч чат-ботів. Від Facebook представлений Блендербот, а від Pandorabots Кукі. Головним завданням так званої "Битви ботів" було перевірити чи зможуть вони достовірно відтворити людську розмову. Даний експеримент проводився більше 12 днів, за цей проміжок часу учасники розмову встигли обговорити ряд тем: політику, спорт, релігію та навіть власні захоплення. Проте результати цієї події не були лише позитивними. Наприклад, Блендербот в одному з діалогів заявив, що Цукерберг не очолює Facebook, а взагалі є автором серіалу «Дуже дивні справи». Ще він назвав Гітлера «видатною людиною», який допоміг йому «в скрутні часи». А ще Блендербот зізнався у вбивстві багатьох людей, після чого питав Кукі, як у неї справи. Опираючись на оцінку BBC можна впевнено заявити, що діалог між чат-ботами "містить занадто багато речень, котрим бракує логічного продовження", а самі по собі вони "взагалі не мають між собою чіткого причинно-наслідкового зв'язку та навряд чи хтось повірить в те, що це було спілкування двох людей". Згідно дослідження CCW Digital: 59% експертів в сфері клієнтського сервісу думають, що технології ботів зможуть покращити роботу працівників служби

підтримки, проте можливостей віртуальних помічників замало, щоб повністю замінити людей. Висновком вищезазначеного досліду було обрання п’яти ключових компонентів якісної підтримки. Ось вони: персоналізація, клієнтоорієнтованість, універсальність, якість спілкування та безпека. “Битва ботів” показала, що при низькій якості спілкування потенційним клієнтам буде незручно користуватися чат-ботом та можливо через це покупці вирішать скористатися послугами іншої фірми або компанії.

Розвиток чат-ботів відтепер не новина, а скоріше необхідність. Компанія Juniper прогнозує, що віртуальний помічник зекономить 8 мільярдів доларів до 2022- го року. За статистикою в 2021 чат-боти змогли зекономити 20 мільйонів доларів. До сфер бізнесу в яких цей вид програмного забезпечення має найбільший успіх у використанні даної технології можна впевнено віднести банківську справу. Причина доволі проста – велика кількість простих звернень з питань та банківських рахунків у цьому секторі.

Отже, чат-боти стали стандартом сфери послуг та не перший рік допомагають уникнути непотрібних грошових затрат і недоцільного використання часу. Для того щоб успішно використовувати можливості цих інструментів потрібно завжди пам’ятати про 5 ключових компонентів якісної підтримки: персоналізацію, клієнтоорієнтованість, універсальність, якість спілкування та безпеку. Це один з найкращих шляхів для отримання більшого прибутку та представлення своїх послуг на ринку праці.

Список використаних джерел

1. chatbotsjournal [Електронний ресурс] – Режим доступу до ресурсу: https://chatbotsjournal.com/chatbot-trends-report-2021
2. carrotquest [Електронний ресурс] – Режим доступу до ресурсу:https://www.carrotquest.io/blog/future-of-chatbots/
3. sendpulse [Електронний ресурс] – Режим доступу до ресурсу:: https://sendpulse.ua/ru/support/glossary/retail

4. hromadske [Електронний ресурс] – Режим доступу до ресурсу:: https://hromadske.ua/ru/posts/sejchas-proishodit-pervoe-v-istorii-svidanie-chat-botov-oni-pytayutsya-obshatsya-kak-zhivye-lyudi-no-poluchaetsya-tak-sebe

РОЗРОБКА ЧАТ-БОТА НА МОВІ NODE.JS

Павленко В. С.
valikpost8@gmail.com
Київський національний університет технологій та дизайну
Хотунов В. І.

Інтернет все більше набуває попиту в різних сферах діяльності і житті людини. Завдяки йому ми зменшили рутинну роботу. Також завдяки IT-технологіям було спрощено роботу в побуті, пошук інформації або її обмін став блискавичним, одним із них є соцмережі. Кожен із молодих людей є в таких мережах як: Facebook, Instagram, Telegram, Instagram, Viber, Tiktok.

Великого попиту набувають магазини, які продають товар в соціальних мережах, або приходять повідомлення про покупку адміністратору в такі мережі з сайту. Наприклад: у вас є інтернет магазин, клієнт робить замовлення, раніше приходило повідомлення лише на почту і на сайт в панель адміністрування сайту. Зараз ще можна підключити бота, який вам надійшло повідомлення не тільки на пошту, а й в соціальну мережу, адже листи можуть попадать в спам на пошті.

Node.js

Node.js - це мова програмування заснована на JavaScript V8, застосовується для взаємодії приладів ввода-виводу через API запроси. Основна роль на сервері - web-сервер, також можна розробити віконні програми. Завдяки тому, що в основі даної мови лежить асинхронність і подієво-орієнтійність, велика перспектива використовувати дану мову для створення чат-бота [1].

Чат-бот

Чат-бот - це програма, яка має штучний інтелект для розмови з співрозмовником, предназначений для полегшення клієнта з взаємодією

комп’ютера. Дана програма може вдосконалюватися в розмові з клієнтом і поліпшувати його пошук і запити по його проханню. Найбільше застосування приходить в нерухомості, коли клієнт фільтрує в переписці всі варіанти товарів і може задати відразу питання менеджеру, якщо є функція зв’язатися з менеджером і менеджер відразу покаже все, що вибрав клієнт.

Також чат-бот може автоматично зробити розсилку всім клієнтам, підписуватись на майбутніх клієнтів, приймати заказ, та ін. В Telegram можна знайти любого бота за вашими потребами.

Перші боти з'явилися в турагентствах, адже там був простий фільтр, який допомагає у виборі путівки [2].

Шкідливе використання:

- спам-боти;
- отримання конфіденційної інформації;
- надсилання вірусів;
- DDoS-атаки;
- ботнери.

Telegram бота з використанням Node.js

Для підключення до Telegram бота треба отримати від Telegram ключа і встановити його в код бота.

Завдяки Node.js можна робити безліч асинхронних запити, швидко обмінюватися і обробляти інформацію. Адже, клієнту важливо отримувати інформацію, яка йому потрібна, створити онлайн оплату і покупку електронного товару не виходячи із соціальної мережі, а найголовніше, завжди під рукою у вас є діалог і пошук вашого товара. Також бібліотеки, які допомагають штучному інтелекту аналізувати потреби клієнта.

Переваги Node.js:

- легке налаштування серверної частини;

- працює 24/7 замість оператора, що економить час роботи оператора в нічний час;
- швидке оновлення інформації;
- низькі вимоги технічної частини сервера;
- велика документація з роботою, як самого Node.js, так і з роботою Telegram.

Недоліки – це оновлення Telegram і оновлення вимог до всіх ботів, які працюють з ним.

Висновок

В даний час чат-боти стрімко розвиваються і охоплюють велику кількість галузей. Все розпочиналося з простого фільтра путівок, а зараз вони в лікарнях допомагають вибрати відповідного лікаря; в банках - інструкцію, або більш чітко зв'язатися з менеджером, який вас може проконсультувати; в магазинах - оформити замовлення, або бути проінформованим про акції, розіграші.

Дана галузь IT-технологій тільки набуває розвитку і ми можемо її вдосконалювати завдяки машинному навчанню і штучному інтелекту.

Література

1. Node.js [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Node.js
2. Чат-бот [Електронний ресурс] – Режим доступу до ресурсу: https://www.sas.com/ru_ru/insights/articles/analytics/what-are-chatbots.html

Секція 2.

Виклики робототехніки в сьогоденні

ЩОДО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ ТА СВІТІ

Носацький К.В.
kostyaa.nosatskiy@gmail.com
Київський Національний Університет Технологій та Дизайну
Оліфіренко В.М.
м. Черкаси, Україна

На сьогоднішній день штучний інтелект та питання роботизації світу це вже не футуристична фантастика, а реальна картина світу. Інновації та автоматизація всіх ланок суспільства від виробництва до розваг стають ключовими рушіями трансформації та діджиталізації суспільства. Вже є достатньо сфер в яких люди співпрацюють із роботами, автоматизованими системами або штучним інтелектом в повсякденному житті пліч-о-пліч.

До найрозвиненіших систем можна віднести наступні:

- Медицина – штучний інтелект вже зараз доволі швидкими темпами заходить в цю галузь, і залишається тільки питанням часу коли він стане буденною річчю в лікуванні людей. Алгоритми та точно налаштовані хірургічні роботи вже сьогодні рятують сотні життів по всьому світі виконуючи надскладні операції де потрібна надточність. І хірургія це не єдина сфера в медицині де проявив себе штучний інтелект, адже його алгоритми добре справляються з діагностикою хвороб. Вчені в шпиталі іменні Джона Редкліффа в Оксфорді винайшли таку систему яка у 80% краще за людей виявляє хворобу серця, дослідники з Гарварду навчили так званий «розумний мікроскоп» бачити небезпечні інфекції в крові.[1]

Розумний будинок – це система розумних пристроїв, яка об’єднана в один вузол, за допомогою якого відбувається управління ключовими функціями будинку.

До головних пристроїв керування можна віднести такі як:

- Смарт-колонки асистенти від Google, Microsoft, Amazon. За допомогою даних елементів можна слухати музику, отримувати інформацію про погоду та актуальні новини, ставити нагадування, вмикати та вимикати світло.

- Робот-пилосос, який прибирає дім без прямої взаємодії з людиною.
- Розумне опалення, яким можна керувати знаходячись на відстані.
- Системи захисту розумного будинку, які передбачають встановлення датчиків, а саме руху, вібрації, відкриття, удару, температури.

Перелік можливостей системи розумний будинок постійно збільшується і розширюється.

Оплата по розпізнаванню обличчя – один з банків України вже впровадив данну функцію у свою систему і дав їй назву FacePay24. Для того щоб нею скористатись потрібно зайти в мобільний додаток і сканувати своє обличчя за допомогою камери.[2]

Чат-боти – Багато хто знайомий з чат-ботами тому що це відносно новий напрям технологій, але він вже став популярний завдяки своїй простоті в використані. Чат-боти використовуються в різних сферах, наприклад за допомогою них можна:

- Завантажити музику з сервісу YouTube.
- Конвертувати відео файли у звукові записи(це може бути корисним для тих хто надає перевагу підкастам).
- Шукати аудіокниги.
- Державна міграційна служба використовує чат-ботів для інформаційної підтримки громадян [3].

І це далеко не повний список того що можуть ці нові гравці у сфері технологій.

Віртуальна реальність (VR) – це створене комп'ютером тривимірне середовище, з яким може взаємодіяти людина. [4]Комп'ютерні ігри стали частиною життя сучасної людини, яка дає новий вид захоплення, а саме кіберспорт та розвиток нових робочих місць для різного роду програмістів та дизайнерів. Станом на 2020 рік в Україні було зареєстровано 180 тисяч IT спеціалістів [5] тому розробка ігор це великий напрям можливостей реалізувати себе та свої здібності як

розробника, так і спортсмена. Є ігри які розвивають малюків або призначенні для реабілітації хворих людей(вони можуть розвивати дрібну моторику, логіку, арифметичні здібності.)

Нові технології та роботизація це наше майбутнє, але разом з тим не потрібно забувати про те що зі зростанням популяризації технологій росте і кількість шахраїв та наших вразливих місць, тому не аби яку роль в розвитку IT сфери є також кібербезпека яка допомагає нам залишатись захищеними у світові павутині.

Література:

1. Савчук . 10 прикладів, як штучний інтелект може змінити ваш спосіб життя [Електронний ресурс] / Тетяна Савчук // https://www.radiosvoboda.org/ – Режим доступу до ресурсу: https://www.radiosvoboda.org/a/29015231.html

2. ПриватБанк. FacePay24 – це швидкий та зручний спосіб оплати [Електронний ресурс] / ПриватБанк // privatbank.ua – Режим доступу до ресурсу: https://privatbank.ua/facepay24.

3. ДМС. Отримайте консультацію з оформлення документів [Електронний ресурс] / ДМС // Державна міграційна служба України – Режим доступу до ресурсу: https://t.me/DMSU_service_bot.

4. Савчук . Можливості технологій віртуальної реальності в різних сферах [Електронний ресурс] / Тетяна Савчук // radiosvoboda.org – Режим доступу до ресурсу: https://www.radiosvoboda.org/a/28903722.html.

5. mind. За 5 років в Україні кількість програмістів зросла вдвічі, а жінок в IT - на 79% [Електронний ресурс] / mind // mind.ua – Режим доступу до ресурсу: https://mind.ua/news/20215670-za-5-rokiv-v-ukrayini-kilkist-programistiv-zrosla-vdvichi-a-zhinok-v-it-na-79-globallogic.

СУЧАСНІ ТЕХНОЛОГІЇ В ГАЛУЗІ АВТОНОМНОГО КЕРУВАННЯ ТРАНСПОРТОМ

Богачов О.П.,
olegbogachov754@gmail.com
Київський національний університет технологій та дизайну
Марченко С.В.
м. Черкаси, Україна

Товариство автомобільних інженерів (SAE) класифікувало транспортні засоби на шість різних рівнів автоматизації. Рівні 0-2 загалом можна віднести до категорії контрольованих водієм, рівні 3 та 4 – назвати напівавтоматичними, а рівень 5 – повністю автономним [1]. Звичайний транспортний засіб можна перетворити на автономний, додавши деякі компоненти, зокрема датчики, що дозволяють транспортному засобу приймати власні рішення, моніторити навколишнє середовище та контролювати рух транспортного засобу [2]. Архітектура транспортного засобу рівня 5 має складатись із чотирьох основних компонентів: моніторинг навколишнього середовища, планування та прийняття рішень, контроль, управління механічними компонентами.

У зв'язку зі збільшенням інтенсивності дорожнього руху підвищується також можливість аварій та зіткнень. Основною метою розвитку автономних транспортних засобів є збільшення безпеки водіння, а також зменшення кількості заторів. Для цього такі транспортні засоби повинні підтримувати зв'язок з іншими транспортними засобами та їх оточенням. Цей процес починається на етапі сприйняття, коли автономний транспортний засіб збирає інформацію із навколишнього середовища за допомогою різних датчиків. Після аналізу навколишнього середовища та прийняття рішення, спеціальна топологія мережі дозволяє автономному транспорту взаємодіяти між собою та з мережевою інфраструктурою для забезпечення дорожньої безпеки та руху транспорту.

Автомобільні самоорганізовані мережі VANET є новим підкласом мобільних спеціальних мереж, здатних до спонтанного створення мережі транспортних

засобів [3]. VANET можна використовувати для зв'язку між транспортними засобами (V2V) та транспорту з інфраструктурою (V2I) [4]. Основна мета такої технології – забезпечення безпеки на дорогах.

Для досягнення автоматизації рівня 5, транспортні засоби повинні підтримувати обмін інформацією з іншими транспортними засобами та оточуючим середовищем. Для досягнення цієї можливості безпілотні автомобілі повинні пройти перехідний період, у якому їм доведеться співіснувати з наявними неавтономними транспортними засобами. Впровадження вимагає ретельного та поступового планування як на транспортному, так і на інфраструктурному рівні [5].

Для розвитку автомобільної комунікаційної мережі ключовим фактором є створення гетерогенної моделі, в якій різні технології зв'язку можуть бути складені разом для виконання різносторонніх завдань [6]. Для цього технологія виділених комунікацій короткого радіусу дії є найбільш доречною технологією для зв'язку типу V2V, тоді як технологія LTE може бути використана для реалізації зв'язку типу V2I. Тим не менше, є багато відкритих питань, таких як передача даних, управління великими даними, покриття мережі та транспортні хмарні обчислювальні системи, які потребують вдосконалення [7].

З досліджень безпілотних автомобілів від компаній Waymo, Tesla, Ford, BMW [8], можна зробити висновок, що жоден тип датчика не може використовуватися для автономної їзди. Для встановлення датчиків можна взяти два підходи. По-перше, один централізований радар на 360 градусів, а по-друге, спеціалізований розподілений набір датчиків по кузову автомобіля. Дизайн програмного забезпечення буде сильно залежати від обраних підходів. Для отримання інформації на 360 градусів потрібно використовувати щонайменше 6 камер у різному напрямку. Датчики, встановлені на передній частині автомобіля, повинні мати дальність дії більше 10 метрів, тоді як датчики з боків і ззаду можуть мати невелику дальність. Додаткові датчики повинні охоплювати сліпі зони, а також працювати як резервні камери. Лише деякі автомобільні компанії використовують

твердотільний лідар. Як тільки технологія стане стабільною і твердотільні лідари будуть випускатися масово, їх вартість стане нижчою.

Карти значно покращать можливість безпілотних засобів пересуватися містом і більше підходять для системи зору. HD карти – це повна цифрова 3D-копія реальної дороги. Карти потрібно регулярно оновлювати, оскільки автономний транспортний засіб не може будувати свою 3D-карту кожного разу, коли проїжджає дорогу, натомість він отримує картографію дороги з попереднього пробігу. Це зменшить багато накладних витрат і призведе до оптимальної продуктивності.

У галузі автономних транспортних засобів розвиваються три нові основні сектори, а саме програмне забезпечення зі штучним інтелектом і HD картами, спеціальне обчислювальне обладнання (наприклад, NVIDIA та Intel) та датчики. Нині механічні лідари замінюються твердотільними лідарами. Багато компаній-виробників концентруються виключно на сенсорах для безпілотного транспорту. Для підключення до хмарних обчислювальних систем використовуються мережі 4G і 5G, що також покращує продуктивність автомобіля та забезпечує оновлення. Що стосується обчислювальної частини, лише NVIDIA придбала дуже перспективну платформу гетерогенних обчислень. Також компанія Telenav пропонує свій програмний продукт Adaptive Autodrive, а Zoox – систему для частини обчислень, аналогічну до NVIDIA. Подібний підхід можна спостерігати для Intel та інших виробників процесорів.

Список використаних джерел

1. A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges / M. N.Ahangar, Q. Z. Ahmed, F. A. Khan, M. Hafeez. // Sensors. T. 21. – 2021. – №706. – С. 1-33.

2. On the instrumentation and classification of autonomous cars / B. C.Zanchin, R. Adamshuk, M. M. Santos, K. S. Collazos. // IEEE International Conference on Systems. – 2017. – №34148. – С. 2631–2636.

3. Hartenstein H. A tutorial survey on vehicular ad hoc networks / H. Hartenstein, L. P. Laberteaux. // IEEE Communications Magazine. T. 46. – 2008. – №6. – С. 164–171.

4. Sheikh A. S. A Comprehensive Survey on VANET Security Services in Traffic Management System / A. S. Sheikh, J. Liang. // Wireless Communications and Mobile Computing. T.19. – 2019. – №2423915. – С. 1–23.

5. Harri J. Mobility models for vehicular ad hoc networks: a survey and taxonomy / J. Harri, F. Filali, C. Bonnet. // IEEE Communications Surveys & Tutorials. T. 11. – 2009. – №4. – С. 19–46.

6. Gao S. An empirical study of DSRC V2V performance in truck platooning scenarios / S. Gao, A. Lim, D. Bevly. // Digital Communications and Networks. T. 2. – 2016. – №4. – С. 233–244.

7. Future cities and autonomous vehicles: analysis of the barriers to full adoption / [N. E. Bezai, B. Medjdoub, A. Al-Habaibeh та ін.]. // Energy and Built Environment. T. 2. – 2021. – №1. – С. 65–81.

8. Pal B. Recent advances in software, sensors and computation platforms used in autonomous vehicles, A survey / B. Pal, S. Khaiyum. // IJRAR. T. 6 – 2019. – №1. – С. 383–399.

УНІВЕРСАЛЬНИЙ АДАПТЕР КОНТРОЛЮ ТА НАЛАШТУВАНЬ ІНЖЕКТОРНИХ АВТОМОБІЛЬНИХ ДВИГУНІВ

Дорошенко Руслан Сергійович,
Київський національний університет технологій та дизайну
Бурмістров Сергій Владиславович
м. Черкаси, Україна

Модернізація двигунів внутрішнього згорання дає можливість продовжити на ринку експлуатацію автомобілів, що використовують теплові двигуни. Основна проблема теплових двигунів – низький коефіцієнт корисної дії.

Для збільшення ефективності роботи двигунів внутрішнього згорання сьогодні використовуються складні електронні системи під управлінням комп'ютерних систем. Дані системи управляють режимами роботи двигуна і різноманітними виконавчими пристроями, наприклад, подушки безпеки, клімат контроль, спеціалізовані електронні блоки управління [1].

Всі електронні блоки з'єднуються єдиною шиною управління. Розробка спеціалізованого діагностичного пристрою або блоку персонального комп'ютера, що підключається до шини управління дає можливість виконувати діагностику роботи окремих вузлів автомобіля, а також коректувати при необхідності окремі параметри роботи двигуна і інших вузлів автомобіля.

Спеціалізовані діагностичні пристрої визначають параметри двигуна, що поєднують в собі потужність, економічність, надійність і екологічність роботи двигуна. Настройка даних параметрів визначає оптимальні режими роботи двигуна в залежності від вимог конкретного користувача автомобілем.

Швидкість роботи шини дає можливість використовувати навіть повільні порти комп'ютера. Існує велика кількість варіантів схем адаптерів: від простих до дуже складних. Вся діагностика роботи автомобільної електроніки повинна виконуватись безпосередньо з комп'ютера. Для цієї мети потрібно або побудувати спеціалізований пакет програмного забезпечення або використати вже існуючі пакети, наприклад, Motor-tester, Mytester, VagCom і VagTool (діагноста автомобілів Audi, Seat, Skoda, VW), Car Scanner (діагноста автомобілів BMW) CarChat, Freescan (діагностика для Ford, Dodg, Craisler) і ін.

Пристрій призначений для підключення персонального комп'ютера до діагностичного каналу електронного блоку управління автомобіля з метою діагностики і управління його функціями.

Література

1. Диагностика электронных систем автомобилей приборами НПП «НТС». Самара, 2014, 259 с.

РОЗРОБКА ТА ЕКСПЕРИМЕНТАЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ РІЗНИХ КОНСТРУКЦІЙ АНТЕН ДЛЯ ЛОКАЛЬНИХ МЕРЕЖ WI-FI ДІАПАЗОНУ

Коваль Денис Анатолійович,
Київський національний університет технологій та дизайну
Бурмістров Сергій Владиславович
м. Черкаси, Україна

В радіодіапазоні виділений цілий ряд частот, які не вимагають обов'язкової реєстрації при їх використанні комітетом по радіочастотному нагляду, за умови, що передаюча апаратура має вказану обмежену потужність.

Частота 2,4 гГц призначена для імпульсних пакетів передачі даних. Діапазон СВЧ дає можливість в коротких імпульсах закодувати великий об'єм інформації. Потужність передавача, що не вимагає реєстрації, законодавством обмежена 400 мВт.

Прокладання мережі за допомогою дротових мереж в умовах низької густоти заселення є нерентабельною справою. Застосування в реальних умовах при використанні широкополосних антен СВЧ-діапазону дає стабільний радіобмін цифровими даними в умовах приміщення 50-150 м, а в умовах відкритого простору до 250м.

Одним із напрямів збільшення рентабельності безпровідних мереж є використання вузьконаправлених антен. Вони дають можливість розповсюджувати сигнал не рівномірно у всі сторони на 360^0 , а фокусувати сигнал в якусь одну сторону, відповідно збільшивши відстань ефективного зв'язку в цьому напрямку [1].

Метою роботи є розрахунок та практичне тестування вузьконаправлених антен, що використовують різні способи поляризації – плоскою (горизонтальна і вертикальна) або круговою (лівозакручена і правозакручена). За основу взято різні конструкції антен, що практично використовуються та виконано розрахунок їх розмірів для СВЧ діапазону. Вузьконаправлений прийом і передача ґрунтується на явищі додавання когерентних хвиль. Передаючий сигнал на своєму шляху натикається на перешкоду, в результаті чого відбивається. Відбитий і основний

сигнал мають однакову частоту але різну фазу перешкода ставиться на такій відстані щоб обидва сигнали стали в одній фазі в результаті чого сигнал підсилюється. Елементи антени які випромінюють сигнал (приймають сигнал), називаються активним вібратором, елемент – перешкода називається директором, елементи кріплення антени в єдине ціле називаються траверсою. Як правило вузьконаправлені антени повинні мати один або кілька активних вібраторів (кожний вібратор налаштований на певну частоту) та десяток або більше директорів. В залежності від конструкції антени, конструкція активного вібратора та директорів може бути різною. Більша кількість директорів дає більший коефіцієнт підсилення, але при цьому зростає вартість антени.

Практичний експериментальний аналіз ефективності різних конструкцій антен за умови стабільності інших параметрів дав можливість вказати ефективні конструкції антен в залежності від відстані між споживачами та визначити параметри конструкції та умов кріплення антен WI-FI діапазону.

Література

1. Э. Спиндлер. Практические конструкции антен. Перевод с немецкого А. А. Левина, А. П. Сахарова. Берлин, 1988, 451 с.

РОБОТОТЕХНІЧНІ ДОСЯГНЕННЯ УКРАЇНИ

Коваленко Д.Ю.
wrathcell@gmail.com
Черкаський державний бізнес-коледж
Оліфіренко В.М.
м. Черкаси, Україна

Світові лідери ринку робототехніки це Китай, Японія, США, Південна Корея, та Німеччина. Уряди цих країн та інвестори виділяють все більше фінансування на даний напрямок кожного року. Найперспективніші напрямки: штучний інтелект, безпілотники, промислові та медичні роботи, логістичні системи. В Україні поки що немає великих досягнень в цій сфері, але позитивний рух розвитку спостерігається:

є і промислові виробники, і стартапи. Стрімко розвивається освітній сегмент — як комерційні курси, так і безкоштовні заняття.

Компанія Drone.ua представляє техніку різних виробників зі всього світу. Представляє різноманітні сфери: аграрну, енергетичну, нафтогазову, топографічну та ін. Компанія пропонує великий каталог техніки. Також є дрон власного виробництва – дрон літакового типу PD 1900. Дана модель призначена для повітряної зйомки високої якості, а за час безперервної роботи (100 хвилин) може покрити близько 1500 гектарів.

Державний концерн «Укроборонпром» поєднує кілька підприємств-розробників, які створюють бойову роботизовану техніку. Одним з проєктів даного концерну, авторство якого належить компанії «СпецТехноЕкспорт», є БТР «Фантом». Це 6-колісна машина, яка може використовуватися при транспортуванні боє-комплектів та поранених бійців на відстань до 20 км. Управління Фантомом проводиться через захищений радіоканал, або за допомогою волоконного кабелю. Також, розробкою «Укроборонпром» є ANSER – безпілотний авіаційний комплекс, що здатний перебувати в повітрі до 12 годин, і може переносити на собі невелику додаткову вагу. Вага безпілотника становить 23 кг, а управління відбувається з використанням повністю зашифрованих цифрових каналів передачі даних.

Розробники компанії «Механізмус» виробляють роботи-манекени для реклами в магазинах одягу, на виставках. Такі роботи мають 9 керованих суглобів, можуть вітати відвідувачів та танцювати. Працюють вони по таймеру або по датчику руху. Компанія постійно удосконалює роботів, придумує нові можливості та покращує сценарії поведінки. Дані манекени автономні, а щоб замінити сценарій, потрібно перезаписати програму рухів на флешку.

Noosphere Engineering School – серія лабораторій, працюють при ДНУ в Дніпрі і КПІ в Києві. У Інжинірингову школу може прийти кожен, у кого є ідея власного робототехнічного або просто інноваційного проекту, і реалізувати свій

проєкт під керівництвом менторів. Ідея проєкту – допомогти студентам створювати хардверні стартапи.

На базі мережі шкіл робототехніки «Boteon» було засновано «Центр сучасної STEM освіти», метою якого стало покращення якості освіти в Україні, та популяризація інженерно-технологічних професій серед молоді. За допомогою нових підходів, вони сприяють всебічному розвитку особистості дитини та її світоглядних орієнтацій.

Список використаних джерел

1) Ел. дж. https://dou.ua/ - стаття «Робототехніка в Україні»

2) Ел. дж. https://drone.ua/

3) Ел. дж. https://ukroboronprom.com.ua/

4) Ел. дж. https://spetstechnoexport.com/

5) Ел. дж. https://eleks.com/

6) Ел. дж. https://mechanismus.pro/

7) Ел. дж. https://ultimaterobotics.com.ua/

ПЕРЕДАВАЛЬНИЙ ПРИСТРІЙ ВІДЕОСИГНАЛУ В ДІАПАЗОНІ ЕФІРНОГО ТЕЛЕБАЧЕННЯ

Ковальов Денис Олександрович,
Київський національний університет технологій та дизайну
Бурмістров Сергій Владиславович
м. Черкаси, Україна

Телевізійний діапазон радіочастот, незважаючи на використання з початку 40-х років 20 століття, постійно удосконалюється. Деякі стандарти вже не використовуються. Їм на зміну прийшли цифрові стандарти. Наявність різних стандартів передачі зображення не є причиною для їх паралельного використання. [1]

Частоти підібрані так, щоб уникнути явища інтерференції та накладання хвиль радіосигналу. Аналогічно розміщені ретранслятори передачі сигналу. Сусідні

ретранслятори не можуть передавати як сигнал однієї частоти так і сигнали сусідніх частот. Обмеження телевізійного діапазону призводить до того, що всі частоти зайняті телебаченням. Незважаючи на це, для місцевої передачі на невеликі відстані є вільні діапазони, які можна використовувати для власних конкретних потреб, якщо потужність передавача не більше 400 мВт при умові, що діапазон передавача не є сусіднім з офіційною частотою, що використовується в даній місцевості. Радіус дії таких передавачів не більше 50 метрів в ефірі та 100 метрів за допомогою коаксіального кабеля. Суттєвою перевагою даного діапазону є наявність великої кількості стандартної професійної прийомної апаратури. [2]

Метою роботи є розробка універсального пристрою для перетворення відео- та аудіосигналу, які є виходами різноманітної апаратури і передаються за допомогою роз'ємів: S-Video, „тюльпан" в телевізійний сигнал малої потужності телевізійного діапазону. Даний пристрій може бути використаний:

1. Дообладнання іграшок з радіокеруванням відеокамерами та мікрофонами (підводний човен, літак).
2. Створення домофонів приватних будинків.
3. Створення ТБ студії в межах навчального закладу.
4. Створення спеціальних науково-дослідницьких пристроїв, які управляються за допомогою радіоуправління займаються вивченням об'єктів, які недоступні звичайними засобами.
5. Створення систем відеоспостереження.
6. Обладнання автомобілів відеокамерами заднього виду.

Пристрій розроблено для передачі відеосигналу для ефірного телебачення в метровому або дециметровому діапазоні в форматі SECAM. Звичайним приймачем для такого сигналу служить телевізійний приймач або комп'ютер обладнаний ТБ–тюнером.

Література

1. *В. Е. Джакония.* Система цветного телевидения SECAM. М.:«Горячая линия-Телеком», 2002. 640 с.

2. *А. Е. Пескин, В. Ф. Труфанов.* Мировое вещательное телевидение. Стандарты и системы. М.: «Горячая линия-Телеком», 2004. 308 с.

РОБОТОТЕХНІКА В НАШОМУ ЖИТТІ

Литовченко В.О.,
група 1К-19, ЧДБК
Ратайчук П.Є.
м. Черкаси, Україна

Штучний інтелект – допоможе людству чи знищить його? Про це сперечаються найвидатніші вчені та розробники. Винахідник Ілон Маск, фізик Стівен Гокінґ, голова корпорації «Майкрософт» Білл Гейтс застерігають від розробки штучного інтелекту, але інші вчені і відомі особистості, такі як Марк Цукерберг, програміст і засновник мережі Фейсбук, навпаки бачать користь для всього людства у застосуванні штучного інтелекту. *Робот* – це електромеханічний, пневматичний, гідравлічний пристрій, програма, чи їх комбінація, яка працює без участі людини.

З кожним роком роботи удосконалюються і розумнішають, але все ж їх штучний інтелект не зрівняється з людським.

Розглянемо топ-5 оригінальних роботів сучасності:

1) Робот-модник

Цей робот створений для того, щоб наочно показати, як одяг, який сподобався користувачу, на ньому виглядатиме. Робот створений з фрагментованих шматків, кожен з яких здатний міняти місце свого розташування. У результаті робот може змінити власні розміри від мінімального до максимального. Цей робот створений стараннями естонських розробників.

2) Робот, який миє волосся від Panasonic

Звичайно, цього робота практичним не назвеш - адже це так нескладно, помити власне волосся, або доручити цю відповідальну справу перукареві. Що ж, якщо людині подобаються сучасні пристрої, ймовірно, йому сподобається і цей робот, який здатний запам'ятовувати індивідуальні характеристики людини, застосовуючи ті процедури для його волосся, яке необхідне саме цьому індивідуумові. Робот сканує голову, переводить все це в 3D-модель для визначення оптимальної кількості шампуню або масажних процедур, які робот теж уміє робити.

3) Робот-бармен з Lego

Цей робот вміє змішувати коктейлі і робить це добре. Робот розуміє мову, так що здатний прийняти будь-яке замовлення, якщо вимовити його досить виразно.

4) Робот-нейрохірург

Це один з найбільш досконалих апаратів сучасності. Для того, щоб створити робота, який дійсно здатний провести складну операцію на мозку, необхідно було витратити безліч часу і грошей. У результаті робот-хірург вже готовий і недавно провів свою першу операцію, видаливши пухлину з мозку пацієнтки. Операція тривала 9 годин, і пройшла вельми успішно.

5) Cubinator

Робот, який швидко складає найзаплутаніший Кубик Рубика, він здатний робити це – всього за 18,2 секунди. Робот в 2010 році потрапив в Книгу Рекордів Гіннеса.

Розглянемо сфери діяльності в медицині в яких доцільно використовувати роботів:

1) Роботи - кур'єри

Стануть в нагоді медустановам і спеціалізовані «кур'єри», які будуть розвозити ліки, інструменти, білизну, їжу і все інше, що тільки може бути перевезено. Одні з найбільш відомих таких машин - TransCar LTC 2 (платформа, на яку можна поставити в тому числі об'ємні контейнери) або Tug (нагадує пересувний шкаф).

У свою чергу, Omnicell M5000 оптимізує роботу з ліками. Часто хворим призначається кілька препаратів одночасно, і дана машина формує відповідні «набори» для кожного пацієнта на кілька днів, розкладаючи таблетки і капсули по блістерах. Швидкість Omnicell M5000 - 50 наборів на годину, тоді як у фахівця-людини в середньому - 4 набори на годину. Пацієнтам робот допомагає тим, що фасує ліки згідно з призначенням лікаря на декілька днів.

Цей пристрій – чудовий приклад, як інтелектуальна робототехніка може взяти на себе рутинні завдання, щоб звільнити людям час для чогось більш важливого.

2)Використання роботів у хірургії

Звичайно, застосування роботів в медицині доцільно і в тих випадках, де потрібно виключно тонка робота. Інтелектуальні пристрої здатні зробити лікування ефективнішим і менш травматичним для пацієнта, знизити ризик розвитку ускладнень. Одна з найбільш «роботизованих» областей медицини - хірургія. Роботи в буквальному сенсі стають руками лікарів, беручи участь в складних операціях.

Мабуть, найвідомішим і високотехнологічним роботизованим хірургом можна назвати систему da Vinci. На даному етапі робот не оперує сам, а лише підпорядковується командам лікаря. Останній сидить за спеціальної консоллю і управляє машиною за допомогою джойстиків і педалей. За роботою він спостерігає через спеціальний екран, куди виводиться багаторазово збільшене 3D-зображення в HD-якості. Ще один асистент перебуває у самого робота і допомагає перемикатися між інструментами. Завдання медичних роботів da Vinci дуже широкі: з їх

допомогою проводяться операції (в тому числі складні і нетипові) на серці, щитовидній залозі, на органах таза та черевній порожнині. Систему da Vinci активно використовують лікарі багатьох країн.

3)Роботи - секретарі

Як і в багатьох інших сферах, робототехніка в медицині допомагає лікарям з рішенням однотипних завдань, що віднімають багато сил і часу, але які не потребують значних розумових зусиль або прийняття рішень. До таких можна віднести реєстрацію пацієнтів, роботу з електронними картами, надання довідкової інформації. Роботів-секретарів вже зараз розроблено чимало, і використовуються вони в самих різних галузях. Цілком ймовірно, що в майбутньому інтелектуальні роботи візьмуть на себе значну частину адміністративної роботи в медичних установах.

Позитивний вплив на життя людини від впровадження роботів:

1. Роботи можуть працювати в суворих і небезпечних кліматичних умовах, їх використовують при розробці родовищ корисних копалин.
2. Використання роботів при виконанні типових дій.
3. Оскільки самі по собі роботи є продуктом високих технологій, то їх розробка і впровадження у виробництво вимагає розробку цілої галузі науки і промисловості, що дає велику кількість робочих місць. Знання, отримані при розробці роботів, зможуть бути застосовані в самих різних сферах.

Негативний вплив на життя людини від впровадження роботів:

1. На сьогоднішній день багато науковців стурбовані що до впровадження роботів в наше персональне життя, а особливо це стосується “ хатніх роботів” , які зможуть зібрати персональні дані про будинок та користувача та передати їх стороннім особам.
2. Не менш важливим є питання, сприйняття людиноподібних роботів в якості живих організмів.

3. Швейцарський аналітичний центр передбачає, що до 2022 року через роботизацію можуть зникнути 75 млн робочих місць.

За прогнозом інших науковців досягнення в області обчислювальної техніки дадуть приблизно 133 млн нових робочих місць.

Тож питання про користь чи небезпеку роботів залишається відкритим.

Південна Корея має найбільшу кількість роботів на душу населення, ніж будь-яка країна світу. На відміну від країн Заходу, технічно-освічені і прагматичні корейці бачать у штучному інтелекті не загрозу людству, а суттєву поміч.

Хіросі Ісігуро – це японець, який створює роботів, відомий тим, що розробляє реалістичних андроїдів, створив нового робохлопчика, який виглядає на 10 років і копіює міміку людини. Міміка андроїда фактично повторює людську, плюс додані мимовільні рухи, які робить звичайна людина – моргання, рух головою і очима. У робохлопчика прозорий «череп». Професор вважає, що важливо створювати таких роботів, тому що, колись роботи стануть частиною нашого життя.

Винахідник думає, що людиноподібні роботи стануть дійсно інтегрованими в суспільство – не тільки для автоматизації виробництва або в якості працезберігаючих пристроїв, але і в якості заміни для фізичної присутності людини. В майбутньому, андроїди можуть стати настільки важливими у нашому житті, що ми не зможемо відрізнити їх від самих себе.

Висновок: Майбутнє наступає вже зараз і необхідно відвести роботам правильне місце в нашому житті, щоб потім ми не відчули їх перевагу над нами.

Література:

1) Що таке робототехніка?: URL: https://academyua.com/ua/stati/32-shcho-take-robototekhnika
2) Інтелектуальні машини: URL: https://www.everest.ua/robototehnika-dlya-osoblyvo-nebezpechnyh-robit/
3) R*obotika*: URL: https://robotica.in.ua/

РІДИННА СИСТЕМА ОХОЛОДЖЕННЯ СИСТЕМНОГО БЛОКУ

Медушівський Олег Костянтинович,
Київський національний університет технологій та дизайну
Бурмістров Сергій Владиславович
м. Черкаси, Україна

Однією з проблем під час проектування системних блоків обчислювальних техніки є охолодження її елементів. Використання пасивного охолодження не є ефективним внаслідок великих розмірів та об'єму радіаторів охолодження. Активні комбіновані повітряні системи охолодження є джерелом низькочастотного шуму. Дані системи не є комплексними. Вони використовуються точково – кожна охолоджує конкретне джерело тепла. [1]

Метою даного проекту є створення комплексної системи охолодження системного блоку на основі застосування рідинної системи охолодження. Даний напрямок є перспективним – система є ефективною з точки зору тепловідведення та одночасно безшумною. Вона повинна охолоджувати всі джерела тепловиділення в системному блоці одночасно – процесор, відео карту та блок живлення.[2]

Дана система не є універсальною. Вона розробляється під конкретну конструкцію системного блоку та відповідне наповнення його апаратним забезпеченням.

Система повинна враховувати фізичні закони теплового руху рідини та наявність активних систем охолодження в точці, де рідина має найвищу температуру. Дана точка повинна знаходитись вже за межами системного блоку на основі ефекту Пельтьє. Для охолодження рідини планується використовувати радіатори, розміщені на зовнішній стороні системного блоку.

Для збільшення ефективності системи крім конвекційного руху рідини планується застосування примусового руху рідини в системі.

Результатом роботи є тривимірне зображення комплексної системи охолодження.

Література

1. Яворский Б. М., Детлаф А. А. Справочник по физике: для инженеров и студентов ВУЗов. — Изд. 4-е, перераб. — Наука - Главная редакция Физико-математической литературы, 1968. 417 с.
2. Скотт Мюллер. Модернизация и ремонт ПК. 19-е издание. Москва: Издательский дом “Вильямс”. 2011. 1072 с.

ОБЛАДНАННЯ ДЛЯ ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ ДРОТОВИХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Овсієнко Олександр Володимирович,
Київський національний університет технологій та дизайну
Бурмістров Сергій Владиславович
м. Черкаси, Україна

Мережеві тестери — пристрої, призначені для перевірки працездатності механічної частини дротових локальних обчислювальних мереж. Дані пристрої призначені для виявлення обривів, замикань, переплутаних провідників, та відстаней до них.

Для спрощення роботи техніка з обслуговування та експлуатації комп’ютерних систем та мереж потрібен нескладний за будовою, простий у користуванні прилад, який зможе швидко і зрозуміло представити інформацію про тестовану дротову лінію. [1]

Для простоти в роботі прилад повинен складатися із двох блоків – перший блок, виготовлений в окремому корпусі, генератор імпульсів, призначений для формування сигналів, що подаються на провідники мережі та індикатора, що отримує сигнали. Генератор по черзі на кожну жилу кабелю повинен подавати електричний імпульс, а з іншої сторони кабелю на індикаторі буде відображено стан кожної жили. Почергове вмикання світлодіодів на індикаторі повинно свідчити, що кабель цілий. Якщо ж вмикаються не всі світлодіоди, це свідчить про розрив на цих жилах. Одночасне вмикання двох світлодіодів свідчить про замикання жил.

Для використання даного приладу достатньо підключити дві його частини на тестованний кабель, увімкнути генератор і отримати інформацію з індикатора.

В процесі виконання дипломної роботи було проаналізовано фізичне середовище передачі даних мережі (кабель вита пара), можливі проблеми при роботі з мережею та методи їх вирішення. Також були проаналізовані прилади для тестування мережі. З усіх існуючих приладів, на даний момент, найбільш функціональними є мережеві тестери, які не тільки проводять тест на цілісність, та правильність обробки кабелю, а й показують відстань до розриву або перемикання. Єдиним недоліком таких приладів є ціна. Аналізуючи недорогі прилади – мультиметри, можна сказати, що недоліком їх є складність перевірки. Тому проаналізувавши потреби монтажників мереж, а саме монтажників «домашніх» мереж можна зробити висновок, що їм потрібен недорогий, надійний, легкий у користуванні пристрій. Цей пристрій повинен перевіряти лінію на розриви, перемикання і переплутані пари.

Були розглянуті найтиповіші проблеми при роботі з кабелем вита пара і розроблені алгоритми їх пошуку.

Для перевірки провідників на обрив достатньо подавати струм на контакти, а з іншої сторони приєднати індикатор який при вмиканні буде вказувати що дана жила ціла, або якщо він не ввімкнувся, то це означатиме обрив.

Для тестування на перемикання жил також достатньо подавати напругу на жили на одному кінці, а на іншому, за допомогою індикатора, дивитися які жили «світяться» одночасно. Це і означатиме перемикання провідників.

Для того, щоб перевірити правильність розводки провідників потрібно по черзі подавати напругу на всі провідники, а на іншому кінці кабеля за допомогою індикаторів спостерігати у якому порядку вони вмикаються. Якщо порядок такий самий, це означає правильне розводки провідників.

Метою проекту є розробка технологічної та конструкторської документації пристрою в двох варіантах – на основі радіодеталей вітчизняного та радіодеталей

імпортного виробництва.

Література

1. Огляд тестера телекомунікаційних мереж та ліній передачі даних Pro'sKit MT-7068. https://masteram.com.ua/uk/articles-and-video/toner-and-probe-kit-mt-7068-rewiev/

СИСТЕМА ЖИВЛЕННЯ НОУТБУКА ВІД АКУМУЛЯТОРА АВТОМОБІЛЯ

Подолян Владислав Русланович,
Київський національний університет технологій та дизайну
Бурмістров Сергій Владиславович
м. Черкаси, Україна

Попит на ринку комп'ютерів на ноутбуки переважає попит на звичайні комп'ютери. Однією із суттєвих переваг ноутбука є його портативність. Одночасно дана перевага є і його слабим місцем. Термін дії електричної батареї є досить обмеженим як і від зарядки до зарядки так і по загальному терміну експлуатації. Різні фірми-виробники електричних батарей виготовляють як правило батареї вказаних типів – свинцево-кислотні, літій-залізо-фосфатні, літій-полімерні, літій-іонні.

Свинцево-кислотні моделі є низькими за собівартістю, можуть працювати при низьких температурах, є невибагливими і безпечними до умов експлуатації. Але вони мають велику вагу, є досить чутливими до глибокої розрядки, мають малий термін експлуатації. Акумуляторна батарея звичайної конструкції може витримати до 300 циклів зарядки-розрядки і до 800 циклів поліпшеної конструкції. Як правило, таких батарей вистачає на рік експлуатації ноутбука.

Літій-полімерні моделі є досить дешевими за собівартістю, мають малу вагу і великий струм віддачі. Вони витримують від 4 000 до 5 000 циклів зарядки-розрядки. Але вони вимагають дбайливого ставлення, досить чутливі до низьких температур, мають низьку пожежостійкість. Саме останній недолік є причиною їх вибухів. Тому використання даного типу на ноутбуках є обмеженим.

Літій-іонні моделі коштують дорого. Вони є чутливими до низьких температур, є досить важкими. Але вони мають найкращі експлуатаційні характеристики і є найбільш привабливими в установці. [1]

Літій-залізо-фосфатні батареї є досить важкими, але легше свинцевих акумуляторів, не бояться низьких температур, мають хороші експлуатаційні характеристики. Але вони вимагають спеціальних умов зарядки-розрядки, мають спеціальну конструкцію батареї.

Ємність батареї забезпечує роботу ноутбука від 1,5 до 3 годин активної роботи. Якщо потрібно використовувати ноутбук постійно в дорозі, виникає необхідність його підзарядки від автомобільної мережі. Більшість ноутбуків живляться від джерела напругою 19В, що робить неможливим їх безпосереднє живлення від бортової мережі автомобіля 12В. Тому виникає необхідність створення спеціального адаптера, який дозволяє підключати ноутбук до електромережі автомобіля. Він повинен живитись від напруги 12В постійного струму та формувати напругу живлення ноутбука 19В та забезпечувати відповідну потужність пристрою. Пристрій повинен бути невибагливим до умов експлуатації та перепадам електроживлення в автомобілі.

Метою проекту є розробка адаптера, що дає можливість працювати ноутбукові від мережі живлення автомобіля. Складність пристрою полягає в тому, що потрібно перетворювати постійну напругу меншого значення в постійну напругу більшого значення. Дана розробка повинна дати можливість використовувати автомобільні акумулятори як джерело живлення ноутбуків, що є альтернативою використання акумуляторів ноутбуків.

Література

1. В. И. Назаров, В. И. Рыженко. Инвертор. Теория и практика. Москва: Оникс, 2008, 40 с., илл.

ROBOTICS IN EDUCATION NOWADAYS

Tarasenko A. V.,
anna0205t@gmail.com
Simon Kuznets Kharkiv National University of Economics
Vasilyk S. K.

Everything changes and technology is no exception. Nowadays, the most popular and needed theme is robotics. This is the base for learning the technical skills needed right now. Robotics is an interdisciplinary branch of engineering and science that includes mechanical engineering, electronic engineering, information engineering, computer science, and others. Robotics deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing. First of all, robots are a big leap forward in education. This technique opens up new opportunities for all students. It is able to teach many skills:

-understand how mechanisms work;

-learn computer basics;

-programming;

- use English language;

-use knowledge in life (math, physics, draftsmanship etc.);

-teamwork skills.

In addition, it will develop creativity, logical thinking, competitive spirit, concentration and attention levels.

Now children are not interested in learning, they believe that school subjects will not be needed in life and won't learn exact sciences because for them such lessons are boring and uninteresting. Robotics is a perfect way to show students that engineering and IT can be fun by making abstract knowledge concrete. Thanks to robotics, learning will be existing and interesting. Pupils will also use knowledge in life that will motivate them to learn better. Parents will not force children. They themselves want to learn how to make a new invention.

A spectacular example of this is yearly festival «Ferrexpo robot fest» which takes place in a small town Horishni Plavni (Komsomolsk) of the Poltava region. The competition has been held for the fourth year already and each time there are more young creative and talented participants. They take part with great relish and learn the fascinating world of robotics.

Such competitions bring up the necessary human qualities. Competing together, children learn the experience of public behavior. Comparing their results with friends, they receive new incentives and begin to make more effort.

Brand manager and expert in robotics company ERC Victor Korotuha writes that it is necessary to integrate robotics with modern learning. In this way, it opens opportunities to study programming and immediately use it in the real world. This develops an interest in learning [1].

Julia Natskevich, an expert at the center of additional education "Snail", considers that robotics can be as an independent discipline at school. Not robotics for school subjects, but school subjects for robotics [2].

Also, there are a lot of advantages in robotics. For example, it's fun for pupils, it gives knowledge for future jobs market. And one of the most important – robots are a great help for autistic children. Now robots are being specially designed for this purpose. The Nao robot, for example, has been helping kids with autism learn social cues, as well as different educational lessons for a few years with a fair amount of success [3].

Exact sciences and robotics are more and more interesting for children. Many educational centers are now introducing the basic principles of robotics to children at a very early age. Today in Ukraine there are 9 school studios, where children study robotics, 3D printing and programming. Such schools have already existed in Kiev, Poltava, Odessa, Lviv, Kharkiv, Dnipro etc. In these courses, children not only create a robot, but also teach it to move, to see, to hear. They also learn basic programming languages and much more.

Thus, robotics will become an inherent part of our life, and soon our existence cannot be imagined without such technology.

References:

1. Robotics and programming as tools in the education of the younger generation, 2018. [Online]. Available: https://ain.ua/2018/05/04/robototexnika-kak-instrum ent-v-obrazovanii/.
2. Do you need robotics at school? The opinion of experts and readers, 2018. [Online]. Available: http://edurobots.ru/2018/05/robototexnika-v-shkole/.
3. The Use of Robotics in Education. [Online]. Available: https://novakdjokovicfoun dation.org/use-robotics-education/.

Секція 3.

Розвиток сучасних проблемно-орієнтованих додатків

НОВІТНІ ІНСТРУМЕНТИ ПЛАТФОРМИ GITHUB ДЛЯ УПРАВЛІННЯ РОБОЧИМИ ПРОЦЕСАМИ ТА ДАНИМИ

Солом'яний Ярослав Сергійович,
soman74geeev@gmail.com,
Черкаський державний бізнес-коледж,
Марченко Станіслав Віталійович

Платформа GitHub – одна з найпопулярніших платформ для командної розробки програмного забезпечення. Вона об'єднує в собі управління проектами, дозволяє планувати нові проекти, створювати окремі гілки проекту, не вносячи корективи в основу проекту, надає можливість працювати з іншими людьми з усього світу. GitHub є одним із найбільших онлайн-сховищ для спільної роботи. До її новітніх інструментів розробки програмного забезпечення можна віднести наступні технології:

–GitHubClassroom– програмне забезпечення, яке має на меті забезпечити можливість для студентів працювати та подавати свої завдання через Git та GitHub, одночасно даючи викладачам можливість представити інструменти контролю версій як частину навчального матеріалу. Використання GitHubClassroom в освітніх умовах включає в себе необмежену кількість приватних репозиторіїв для студентської роботи. Оскільки це новий інструмент, немає добре задокументованих і простих опублікованих робочих процесів, в яких описано, як найкраще використовувати GitHubClassroom. Керівник курсу може надавати групі окремі матеріали для виконання завдань студентами на відміну від індивідуального завантаження завдань для кожного індивідуально. Студенти в свою чергу можуть використовувати Gitдля завантаження виконаних завдань для їх подальшої перевірки системою.[1].

Клас GitHub можна легко використовувати для надання зворотного зв'язку з кодом під час навчання студентів. GitHubClassroom дозволяє робити кожне завдання приватним, натискаючи лише одну кнопку. Кожний студент (або команда) може переглядати лише власні репозиторії, у той час, як викладачі мають доступ до всіх

репозиторіїв. Викладачі не лише мають спосіб запобігти обману (домашні завдання не переглядаються загальнодоступно і не копіюються), але також дотримуватися правил конфіденційності. Якщо студенти хочуть поділитися своєю роботою з потенційними роботодавцями, вони можуть легко зробити свої репозиторії загальнодоступними[2].

GitHubActions – універсальний інструмент для автоматизації запуску коду в результаті настання певної події. Реліз інструменту відбувся 13 листопада 2019 року. Налаштування робочих процесів здійснюється у вигляді YAML-файлу, що необхідно зберігати в репозиторії по шляху .github/workflows. Вміст такого файлу зазвичай складається з кількох базових зіставлень: опція name визначає назву дії для відображення в інтерфейсі GitHub; опція on відкриває секцію тригерів для запуску коду; опція jobs визначає список операцій (з кроками – steps), які слід здійснювати в якості реакції на настання події. Крім того, доступні й інші зіставлення: uses для повторного використання готових дій, with для параметризації кроків, причому параметри регламентуються власне дією, run для запуску команди в shell-терміналі та ін. Документація платформи детально описує різновиди тригерів, які групуються в наступні категорії: події робочого процесу, заплановані події, мануальні події та події-вебхуки. Також запустити реакцію на подію можна за допомогою персонального токену доступу [3].

Таким чином, використовуючи GitHubActions, можна автоматизувати запуск різноманітних операцій у відповідь на push чи pullrequest, створення нового репозиторію, завершення роботи таймеру тощо. Код обробників таких подій зазвичай запускається на віртуальних машинах платформи GitHub, проте також можна налаштувати запуск на власних віртуальних машинах. Універсальність інструменту полягає в довільності реагування на події: можна виконувати прогони тестів, збирати та розгортати програмний продукт, сповіщати людей, збирати статистику та ін. [4] У результаті поширеним застосуванням GitHubActions є

конфігурування простого безкоштовного CI/CD-пайплайну, що особливо актуально при використанні DevOps-підходу в розробці програмного продукту.

GitHubCodeSpaces – це середовище розробки, інтегроване в платформуGitHub.На даний момент перебуває на стадії бета-тестування. Працює на основі VisualStudioCode. Кодовий простір включає в себе все необхідне для розробки конкретного сховища, включаючи текстовий редактор з підсвічуванням синтаксису та автозаповненням. Інтерфейс програми містить Термінал, інструменти налагодження та команди Git.

Codespaces полегшує розробникам перехід в нову компанію або початок участі в проекті з відкритим вихідним кодом. Супровідникипроєкту можуть налаштувати репозиторій таким чином, щоб при створенні кодового простору для репозиторію залежності проекту включалися автоматично. Це дає змогу почати кодування швидше, скоротивши час на налаштування середовища. Можливе встановлення розширення коду VisualStudio в своєму кодовому просторі, щоб додати більше функціональності. Codespaces полегшує розробникам перехід у нову компанію або початок участі в проекті з відкритим первинним кодом. Кожен розробник може створити один або кілька кодових просторів для будь-якого публічного чи приватного репозиторію, що належить до його облікового запису[5].

Вище згадані технології показують високу динаміку розвитку платформи. Це може бути зумовлено ще й нещодавнім придбанням платформи компанією Microsoft, яка вже має досвід розвитку вебхостингу для програмних проєктів (колишній CodePlex) та значні фінансові ресурси. Очевидним є прагнення компанії зробити зі свого сервісу повноцінне онлайн-середовище для розробки та управління програмними проектами, розширити галузі застосування платформи ще й в освітньому середовищі.

Список використаних джерел:

1. Howtogradeprogrammingassignmentsongithub. [Електронний ресурс] / GitHub. – 2017. – Режим доступу до ресурсу: https://education.github.community/t/how-to-grade-assignments-on-github/13663.
2. Using GitHub Classroom To Teach Statistics / [J. Fiksel, J. Hardin, L. Jagertaін.]. // Journal of Statistics Educations. – 2018. – С. 1–20.
3. Eventsthattriggerworkflows [Електронний ресурс] – Режим доступу до ресурсу: https://docs.github.com/en/actions/reference/events-that-trigger-workflows.
4. Githubactions: базовыепонятия [Електронний ресурс] – Режим доступу до ресурсу: https://cakeinpanic.medium.com/github-actions-%D0%B1%D0%B0%D0%B7%D0%B0 -2501445e7392.
5. GitHubCodeSpaces [Електронний ресурс] – Режим доступу до ресурсу: https://docs.github.com/en/github/developing-online-with-codespaces/about-codespaces.

СИСТЕМА АВТОМАТИЗАЦІЇ ДЕКЛАРУВАННЯ РОБОЧОГО ЧАСУ IT-СПЕЦІАЛІСТА «SMILE-TRACK»

Вакуленко Д.В.
Київський національний університет технологій та дизайну,
Захарова М.В.

Облік робочого часу відведеного на виконання задач IT-фахівця ведеться за допомогою фіксування часу тайм-трекером. Це є однією з вимог від співробітників аби контролювати їхню ефективність. Деякі фрілансери навпаки фіксують свій робочий час з власної ініціативи – щоб збільшити продуктивність, а також краще оцінювати вартість своїх послуг, або не перепрацьовувати.

Останнім часом набирає популярність використання програм тайм-трекерів при роботі з віддаленими співробітниками і найманими працівниками

(програмістами, бухгалтерами, дизайнерами, фахівцями служб підтримки та іншими), що працюють за схемою погодинної оплати праці [1].

Тайм-трекер (англ. Time-tracker або Time-tracking software) — це категорія комп'ютерного програмного забезпечення, що дозволяє співробітникам, які працюють за комп'ютерами, фіксувати час, витрачений на виконання завдань або проектів, а роботодавцям їх контролювати [2].

Система «Jira» — комерційна система призначена для організації взаємодії з користувачами та для керування проектами, що застосовується в якості інструменту управління проблемами, завданнями, проектами в різних галузях. Для кожного з проектів створює і веде схеми безпеки і схеми оповіщення [3]. Система «Jira» працює не досить швидко, тому весь процес додатково затягується із-за проблем із недосконалим користувальницьким інтерфейсом. Кожну задачу потрібно знайти і за допомогою декількох натиснень заповнити всю інформацію, що також займає певний час.

Тобто, саме спрощення полягає у тому, що до цього потрібно було всі задачі окремо шукати в системі «Jira».

Мета: розробка системи, що дозволить вести автоматичний облік виконаних задач та часу, що був витрачений на їх виконання.

Робочий день програміста триває 8 годин. Цей час може бути розділений на декілька задач. Оскільки потрібно самостійно вести облік виконаних задач та часу, що витрачено на них, і якщо вчасно не зафіксувати одну з задач, то вона буде втрачена. Підрахунок витраченого часу може бути не точним, оскільки для точного ведення часу потрібно постійно перевіряти й постійно фіксувати прогрес виконаних задач. Процес фіксації виконаних задач та часу, що витрачено на них, займає багато часу більшість програмістів відчувають проблеми, коли потрібно зафіксувати час. Або вони його фіксують не вірно, або пропускають деякі вже завершені задачі. А деякі програмісти затягують з процесом фіксації виконаних завдань. І потім в кінці тижня вони фіксують весь об'єм виконаної роботи. Але є такі проекти, де є вимоги

фіксувати завершення задач кожного дня. Тобто, виникає проблема обліку виконаних завдань та фіксації витраченого на їх виконання часу.

«Smile-Track» — це утиліта, яка дозволяє автоматично дивитись на які задачі програміст витратив свій час, скільки часу він витратив, а також підтягнути події з гугл-календаря, зустрічі та інші заходи. Фахівець має можливість: переглянути час, який утиліта зібрала; змінити його; відредагувати як потрібно в залежності від задачі; дописати або прибрати деякі коментарі; вибрати задачу, якої потрібно зафіксувати час. Після чого натиснувши одну кнопку «затрекати» ці данні.

Розроблена система «Smile-Track». Оскільки вона є відокремленою розробкою, то швидкість використання є максимально ефективною, а також відсутній потік зайвих даних, і при необхідності є можливість перейти до задач у «Jira», перевірити чи вірно зафіксовано час, або виконати інші необхідні для роботи операції.

Література:

1. Топ-9 лучших тайм-трекеров для учета рабочего времени, обзор и сравнение 2021 года. [Електронний ресурс]. — Режим доступу: https://bit.ly/3amNxBr (Дата звернення: 25.03.21).

2. Данило Голота. Я працюю з тайм-трекером (це текст про надмірний контроль або збільшення продуктивності). – The Village [Електронний ресурс]. — Режим доступу: https://www.the-village.com.ua/village/business/business-ethics/302197-yak-tse-pratsyuvati-z-taym-trekerom (Дата звернення: 24.03.21).

3. Лучший инструмент разработки для agile-команд. Atlassian [Електронний ресурс]. — Режим доступу: https://www.atlassian.com/ru/software/jira (Дата звернення: 24.03.21).

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ МОБІЛЬНИХ ДОДАТКІВ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Біданець Лада Володимирівна
здобувач вищої освіти 2 курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ
Кисельов Андрій Олександрович
доцент кафедри оперативно-
розшукової
діяльності факультету підготовки
фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
майор поліції

Карти кримінологічного прогнозу можуть і повинні розроблятися у тісній співпраці картографів і аналітиків-правознавців, бо лише останні в силу своєї професійної кваліфікації можуть об'єктивно оцінити інформацію інвентаризаційних і оцінювальних карт, які відображають показники, що розраховуються за визначеними, відомими алгоритмами.

Науково-технічний прогрес, без перебільшення, можна вважати способом буття сучасної людини. Ще на зорі розвитку епохи телеграфу і телефону всесвітньовідомий винахідник Томас Едісон зазначив, що первинною умовою прогресу людства є незадоволеність. Вочевидь, й інноваціям у сфері протидії злочинності сприяє саме незадоволеність станом боротьби з цим ганебним явищем [1].

Це природно викликає прагнення всіляко підсилити заходи із запобігання злочинам та бажання підвищити ефективність їх розслідування, адже у такий спосіб можна значно оптимізувати роботу органів поліції у здійсненні кримінального

аналізу , тим самим забезпечивши невідворотність притягнення злочинців до кримінальної відповідальності та їх покарання .

Засновник кібернетики та теорії штучного інтелекту Норберт Вінер якось сказав, що ми змінили своє оточення настільки радикально, що тепер маємо змінювати себе, щоб жити в цьому новому оточенні. Дійсно, в інформаційному суспільстві як постіндустріальній фазі розвитку цивілізації головними продуктами виробництва стають інформація та знання. Дедалі впевненіше суспільство входить в епоху діджиталізації, тобто інформаційної трансформації, яка має забезпечити кожному громадянинові рівні можливості доступу до послуг, інформації та знань, що надаються на основі інформаційно-комунікаційних технологій [1].

Цілком ймовірно, що серед величезної кількості користувачів зустрічаються особи, які не здатні в силу певних відхилень в своїх інтересах, переконаннях або поглядах (в тому числі і негативних) самореалізуватися в суспільстві. Водночас групова згуртованість і постійне спілкування для таких осіб - це основне засіб захисту власних інтересів і взаємної підтримки. Однак подібна згуртованість і спілкування в реальному світі для них вкрай скрутні по ряду причин (важко знайти собі подібних, небажання афішувати свої протиправні переконання та інтереси і тощо) [2]. Соціальні мережі ж надають їм унікальні можливості для організації спільнот протиправного характеру, комунікації з метою обміну суспільно-небезпечним досвідом, а також для здійснення протиправних дій. Визначимо основні загрози, з якими можуть зіткнутися неповнолітні користувачі в соціальних мережах [2].

Так, встановлюючи GetContact, необхідно прийняти умови угоди. А саме та опція, яку все не дивлячись відзначають галочкою. Приймаючи умови договору, ви дозволяєте компанії збирати будь-які дані і ділитися ними з третіми сторонами. Також вона може розпоряджатися відомостями в рамках туманного положення про право «підтримувати і розширювати свої послуги». Ще один пункт відкриває дорогу

для спаму, фіксуючи дозвіл на проведення «маркетингової активності». У неї входить розсилка SMS, електронних листів і навіть дзвінки.

Неповний список інформації, яку отримує GetContact, виглядає так:

інформація з телефонних книг (контакти та інше);

фотографії;

поштова адреса;

IP-адреси;

історія дзвінків.

Нюанс ще і в тому, що навіть не встановлюючи GetContact, ваш номер може виявитися в розпорядженні розробників - досить, щоб він виявився в адресній книзі одного з користувачів [2].

Getcontact LLP (“Getcontact”, “наш,” “ми,” або “нас”) надає комплексний сервіс ідентифікації абонентів, що здійснюють вхідні дзвінки (integrated caller ID service) для активного блокування спаму та небажаних дзвінків, з можливістю інтегрувати Ваш профіль у соціальних мережах та пошуку контактів в нашому каталозі. Будь ласка, прочитайте наші Умови надання Сервісів для того, щоб Ви могли чітко зрозуміти, як ми виконуємо нашу роботу і яку поведінку ми очікуємо від Вас при використанні наших послуг. Ви погоджуєтеся на наші Умови надання Сервісів шляхом встановлення, здійснення доступу до або використання мобільного додатка, функцій, програмного забезпечення або веб-сайту Getcontact (разом - “Сервіси”).

За умови, що Ви дотримуєтеся всіх своїх зобов'язань за цими Умовами, включаючи, але не обмежуючись, Кодекс поведінки користувача (User Code of Conduct), зазначений нижче, ми надаємо Вам обмежену, відкличну, невиключну, що не підлягає передачі або субліцензуванню, ліцензію та право на використання Сервісів Getcontact через мобільний пристрій або додаток [1].

Важливо відзначити, що діяльність Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України так само

пов’язана з розробкою інноваційних методів у справі боротьби зі злочинністю. Так, фахівцями нашої криміналістичної лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю», що розпочала свою роботу ще у вересні 1995 р., та представниками Національного юридичного університету імені Ярослава Мудрого спільними зусиллями розроблено, зокрема, автоматизоване робоче місце слідчого «Інсайт», інформаційно-пошуковий модуль АІПС «Кліше», методика ідентифікації людини за параметрами мовних сигналів; алгоритми автоматизованої цифрової фотозйомки, цифрового відео- та звукозапису; алгоритми ідентифікації людини на основі біометричних ознак та багато іншого.

Отже, таким чином можна сказати, що за допомогою сучасних мобільних додатків можна здійснювати кримінальний аналіз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Пересадько В.А. Картографування кримінологічної ситуації (на прикладі Сумської області) / В.А. Пересадько, Є.В. Орлов // Проблеми безперервної географічної освіти і картографії. – 2015. – Вип. 22. – С. 94-98. [Електронний ресурс]. URL: http://goik.univer.kharkov.ua/wp-content/files/issue_22/22_26.pdf

2. Горбатенко В. Метод «Делфі» та специфіка його застосування у прогнозних розробках / Володимир Горбатенко, Ігор Петренко // Політичний менеджмент. – 2008. – № 6. – С. 174–182. [Електронний ресурс]. Режим доступу: http://www.irbisnbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21RF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FLA=&2_S21STR=PoMe_2008_6_19

3. Овчинский В.С., Ларина Е. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М, 2014.

СПЕЦІАЛІЗОВАНА ЛОКАЛЬНА МЕРЕЖА ПІДПРИЄМСТВА НА ОСНОВІ СЕРЕДОВИЩА „PRO100”

Вінник Максим Ігорович, студент
Київського національного
університету технологій та дизайну
Бурмістров Сергій Владиславович

Використання комп’ютерів та відповідного програмного забезпечення повинно суттєво зменшити собівартість виготовлення продукції на виробництві. Одним із перспективних напрямків застосування ЕОМ є заміна на виробництві підрозділів, які виконують розрахунково-проектні роботи програмним середовищем, в якому враховані всі СНІПи, стандарти, технологічні норми та особливості виробничого процесу підприємства. Застосування комп’ютерів дає можливість значно скоротити кадровий апарат, що автоматично призведе до зменшення податкового навантаження на підприємство, використовувати для тієї ж роботи працівників з набагато нижчим кваліфікаційним рівнем. Використання такого середовища в умовах малого підприємства дає можливість виконувати індивідуальні замовлення споживачів по собівартості масового виробництва. За рахунок зменшення затрат на конструкторську технологічну документацію, чітко контролювати ринок продукції в даній галузі і за рахунок мінімальних капіталовкладень швидко змінювати асортимент готової продукції.

Метою проекту є розробка моделі малого приватного підприємства для виготовлення корпусних меблів під індивідуальні замовлення споживачів з мінімальною собівартістю готової продукції.

На сьогоднішній день виробництво корпусних меблів поставлено на досить солідну промислову основу. Сьогодні малі підприємства, які надають послуги по виготовленню даної продукції, є інтегрованими в загальний процес виготовлення. Вони використовують напівфабрикати, фурнітуру великих підприємств, які займаються масовим їх виготовленням. Технологія є наскільки досконалою, що дає змогу організовувати підприємство складом від двох працівників. При наявності

нескладного обладнання підприємство має змогу виготовляти продукцію, що відповідає стандартам ринку. В результаті ринок насичується продукцією даного виду.

Для успішного ведення бізнесу потрібно враховувати особливості індивідуальних замовлень і швидко реагувати на зміни кон'юнктури ринку в умовах малого бюджету організації. Для організації нової структури підприємства пропонується використовувати програму Pro100, призначену для створення проектів комплексів корпусних меблів та органічного їх розміщення в конкретному приміщенні. Дана програма випущена на умовах тестування з метою виявлення недоліків та погрішностей, які могли виникнути в процесі розробки і розрахована для використання в монопольному режимі на конкретному комп'ютері. Вона не вимагає спеціальних конструкторських, економічних, технологічних знань, що дає змогу користуватися нею, починаючи від менеджерів, які проектують кінцевий результат безпосередньо перед замовником з врахуванням розміщення готового виробу, і закінчуючи робітником, який виготовляє окремі деталі та збирає їх в готовий виріб.

Використання програми вносить свої корективи на створення нового типу взаємозв'язків між відділами маркетингу, виготовлення готової продукції та установка готової продукції.

Література:

1. Pro100. Программа для дизайна мебели и интерьеров. Версия 3.6. Руководство пользователя. Москва: ECRU. 2003, 68 с.

GRAPHQL – ПОЧАТОК КІНЦЯ REST API

Головенко М.Л.,
holovenkomaksyml@gmail.com
Черкаський державний бізнес-коледж
Марченко С.В

Коли заходить мова про мережеві запити між клієнтськими і серверними додатками, найчастіше як місток між ними обирають REST. У такому випадку все розвивається навколо ідеї «нам потрібні ресурси, доступні за URL». Можна зчитувати ресурс за допомогою запиту HTTP GET, створювати ресурс за допомогою запиту HTTP POST, оновлювати і видаляти його за допомогою запитів HTTP PUT і DELETE. Ці операції називаються CRUD (Create, Read, Update, Delete). В якості ресурсу може виступати будь-який контент, отриманий від авторів, користувачів або взяте з статей. При використанні REST формат передачі даних жорстко не заданий, але, частіше за все, для цієї мети використовується JSON. Загалом REST забезпечує комунікацію між додатками за звичайним протоколу HTTP із застосуванням URL і HTTP-методів.

Дуже часто реальні програми можуть зіткнутися з обмеженнями традиційних REST API інтерфейсів. Наприклад уявимо, що потрібно відобразити список записів (posts), і під кожним опублікувати список лайків (likes), включаючи імена користувачів і аватари. З цією метою достатньо просто змінити API для записів так, щоб він містив масив лайків, у якому будуть об’єкти-користувачі. Проте потім, при розробці мобільного додатку, виявилося що через завантаження додаткових даних додаток працює повільніше. Це призвело до потреби в двох ендпоінтах (endpoint): один повертає записи з лайками, а інший – без них. Ситуація може ускладнюватись ще й тим, що записи зберігаються в базі даних MySQL, а лайки, наприклад, в Redis. Екстраполюючи цей сценарій на множину джерел даних і клієнтських API, з якими мають справу реально навантажені системи, стає очевидно, що REST API вже досяг своєї межі.

У компанії Facebook було запропоновано концептуально просте рішення: замість того, щоб мати безліч «дурних» ендпоінтів, краще мати один «розумний». Саме він буде здатний працювати зі складними запитами і надавати даним таку форму, яку запитує клієнт. Фактично, прошарок GraphQL знаходиться між клієнтом і одним або декількома джерелами даних; він приймає запити клієнтів і повертає необхідні дані відповідно до переданих інструкцій [1].

За своєю суттю GraphQL є мовою запитів, зорієнтованою на отримання результатів у формі JSON-даних. Наприклад, розглянемо запит:

```
author(id: "4") {
 id
 name
 avatarUrl
 articles(limit: 4) {
 name
 urlSlug
 }
}
```

Він звертається за множиною ресурсів (автор, стаття), які в GraphQL називаються полями, та конкретним набором вкладених у них полів (name, urlSlug для статті). При цьому, в GraphQL-схемі даних може надаватися й інша інформація (наприклад, для статті – анотація, дата виходу тощо). У той же час, в REST-архітектурі потрібно було б мінімум два запити для витягування суті «автор» і статей цього автора. GraphQL вирішує цю задачу одним запитом. Крім того, при запиті вибираються лише необхідні поля, а не цілком вся сутність. У разі, коли серверний додаток надає схему GraphQL, в якій визначає всі доступні дані зі своєю ієрархією і типами, клієнтський додаток запитує лише ті дані, які йому потрібні.

Можна виокремити наступні переваги використання GraphQL:

1) декларативна вибірка даних;

2) ніякої перевибірки при роботі з GraphQL;
3) GraphQL для React, Angular, Node та ін.;
4) єдине джерело істини – схема GraphQL;
5) GraphQL слідує сучасним тенденціям;
6) сильна типізація;
7) зростаюча екосистема.

До недоліків GraphQL можна віднести такі:

1) складність запитів;
2) неможливість обмеження швидкості запитів;
3) складність кешування [2, 3].

У підсумку можна сказати, що через свою багатогранність технологія GraphQL спочатку може здатися складною. Тим не менше, все більше компаній та структур починають використовувати її, а протягом наступних декількох років GraphQL може стати одним з ключових будівельних блоків у веб-розробці. Серед крупних компаній, що інтегрували GraphQL у свій технологічний стек, вже є такі: Shopify, Github, Medium, Docker, Twitter, Airbnb Paypal та ін. [4].

Список використаних джерел:

1. Что же такое этот GraphQL? [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://habr.com/ru/post/326986/.
2. Введение в GraphQL: преимущества и недостатки [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.8host.com/blog/vvedenie-v-graphql-preimushhestva-i-nedostatki/.
3. Краткий экскурс в GraphQL [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/company/piter/blog/424037/.
4. The 10 Best GraphQL Tools For 2021 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://graphcms.com/blog/best-graphql-tools-2021.

ВИКОРИСТАННЯ СОЦІАЛЬНОЇ МЕРЕЖІ ICQ ПІД ЧАС ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ

Єрохін Артур Олексійович
здобувач вищої освіти 2 курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ
Кисельов Андрій Олександрович
доцент кафедри оперативно-
розшукової
діяльності факультету підготовки
фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
майор поліції

Прийняття нового Кримінального процесуального кодексу України, який відповідав би стандартам Ради Європи, було умовою виконання зобов'язань, взятих нашою державою. Основними напрямами реформування кримінального судочинства, відповідно до Кримінального процесуального кодексу України (далі - КПК України), прийнятого 13 квітня 2012 року є створення рівних можливостей для кожної із сторін у кримінальному провадженні та реальне впровадження у кримінальне судочинство принципу змагальності, за якого результат розгляду судом конкретного випадку притягнення особи до кримінальної відповідальності залежатиме виключно від обґрунтованості позиції сторін та доказів, отриманих на стадії досудового розслідування шляхом проведення гласних та негласних слідчих (розшукових) дій.

Але 2017 рік вніс певні корективи в роботу Національної поліції та навіть полегшив її, було створено Управління Кримінального Аналізу, основним завданням якого стало проведення аналітичних досліджень, в межах оперативно

розшукових та кримінальних проваджень , за запитом відповідних органів та підрозділів.

Активні дискусії точаться з приводу введення такого інституту кримінального провадження як негласні слідчі (розшукові) дії, що фактично викликало появу питання про співвідношення заходів оперативно-розшукової діяльності та негласних слідчих (розшукових) дій у кримінальному провадженні. Наприклад однією з таких негласних слідчих (розшукових) дій є зняття інформації з електронних інформаційних систем.

На сьогоднішній день в системі поліції існує дуже багато джерел розрізненої інформації. Вона аналізується автономно співробітниками різних служб. І все це зберігається в різних базах.

Оперативники накопичують та зберігають всю інформацію у себе, після звільнення, останніх, ця інформація не зберігається.

Створення управління кримінального аналізу допомогло не тільки зберегти відомості відносно досліджуваних об‘єктів але й підвищити цінність такої інформації.

Отриманню такого роду інформації передує ретельна робота з веденням окремої спеціалізованої бази даних із зазначенням необхідних фактичних даних, зокрема з соціальних мереж таких як Viber, Telegram, ICQ та інші.

В мережі ICQ за допомогою втручання в особисту розмову (за умови виконання слідчої дії та з дозволу відповідного органу) можливо дізнатись всю необхідну інформацію яка допоможе у проведенні слідчої дії , розшуку правопорушників та запобіганню вчиненню як кримінальних так і адміністративних правопорушень,

Також за допомогою кримінального аналізу та використання ICQ під час кримінального аналізу, створюються відповідні звіти, досьє, тощо,

зберігається вся інформація про предмет або суб’єкт, наприклад : своєрідного «досьє зброї» в якому зберігається вся інформація про зброю, наприклад:

- серія, номер, індекс;
- марка, модель;
- виробник;
- країна виробника;
- шлях потрапляння в Україну;
- облік МВС чи Збройних сил України, інші правоохоронні органи;
- шлях у руках власників (переоформлення/продаж).

Коли зброя потрапляє в категорію речей, які «важко дістати», працівникам оперативних підрозділів за власною агентурною інформацією та за інформацією яка зберігається в базі даних та в досьє , набагато легше відслідковувати факти появи такої зброї «поза законом».

Крім цього, велика частина людей використовує служби обміну повідомленнями (Месенджери) в тому числі (ICQ) або програми для телефонних дзвінків через Інтернет, які також надають можливості пошуку своїх користувачів. Звичайно, кожен користувач месенджера може заборонити видавати його профіль у пошуку користувачів, але роблять це зовсім не всі.

Запустивши програму на своєму мобільному пристрої або комп'ютері, також можна зробити пошук людей по імені та прізвищу. Найвідоміші програми наведені в (Skype, ICQ, WhatsApp, Viber, Telegram, Snapchat). Також неможливо оминути увагою те, що в мережі Інтернет швидше, аніж працівники поліції встигають такі факти реєструвати, з’являється інформація про новітні способи шахрайств.

Отже, підсумовуючи наведене, слід резюмувати, що сьогодні використання оперативного пошуку в мережі Інтернет, соціальних мережах та електронних месенджерах може надати можливість оперативним працівникам отримувати додатково до 20% первинної оперативно-розшукової інформації, що становить оперативний інтерес. Але через втручання до особистого життя, особистої розмови, суб‘єкти відносно яких проводиться кримінальний аналіз , можуть обжалувати дії

даного Управління та поскаржитись до відповідних інстанцій якщо їм стане відомо про факт відслідковування інформації, розмови та інших нюансів їхнього життя.

На сьогодні проблема захисту прав людини стоїть достатньо гостро як у світі загалом, так і в Україні зокрема. У межах цього дослідження ми зосередимо свою увагу на праві на приватність (ст. 8 Європейської конвенції з прав людини). Це право охоплює широкий спектр питань, до яких належать: сімейне життя; житло; приватне життя, а саме фізична, психологічна чи моральна цілісність, конфіденційність, індивідуальність та автономія; а також кореспонденція. Саме засоби забезпечення таємниці останньої в умовах глобалізації, інформатизації, поширення соціальних мереж цікавлять нас у передусім.

Підрозділи кримінального аналізу, докладають зусиль щоб всі їх дії були законними та відповідали нормам, передбаченим Конвенцією про захист прав людини та основоположних свобод.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Малицька І. Д. Віртуальні спільноти як інноваційні освітні середовища в системах освіти зарубіжних країн. Інформаційні технології в освіті: 2013. № 15. С. 276–283.
2. Никитина Л. Е. Социальный педагог в школе: Академический проект, 2003. 112 с.
3. Олексюк Н. В. Використання соціальних мереж у роботі вчителів: Звітна наукова конференція Інституту інформаційних технологій і засобів навчання НАПН України: матеріали наукової конференції. Київ: ІІТЗН НАПН України, 2015. URL http://conf.iitlt.gov.ua/-Conference.php?h_id=10.
4. Середа Х. Мережа партнерство в навчанні для освітян України: Інформаційні технології в освіті: збірник наукових праць. 2011. №9. С. 70–81.

ЗАСТОСУНОК БЛОКУВАННЯ ДАНИХ ДЛЯ БАТЬКІВСЬКОГО КОНТРОЛЮ

Повжик С. І.
Київський Національний університет технологій і дизайну
Чепинога А. В.

Сьогодні інтернет є невіддільною частиною нашого життя і особливо гостро стоїть питання безпеки його використання. Найбільше це стосується дітей, оскільки на сьогодні вони частіше дорослих займаються веб-серфінгом, проводять час в соціальних мережах та онлайн-іграх. В силу свого віку, дитина не знає, які небезпеки її можуть підстерігати, і тоді на допомогу приходять додатки для батьківського контролю.

Згідно з статистикою [1], вже починаючи з 8-9-річного віку, діти самостійно користуються інтернетом, а кожна п'ята дитина проводить понад 4 години на день в мережі. Якщо брати статистику дітей до 14-річного віку, то більш ніж половина з них відвідують сайти з небажаними матеріалами, 39% продивляються порносайти, а 19% дивляться сцени насилля. Саме діти віком від 12 до 17 років є основною групою ризику для розвитку інтернет-залежності. Все це пояснюється дуже просто: у людей, які проводять понад 9 годин в тиждень за комп'ютерними іграми, відмічалось збільшення об'єму центральної частини мозку, яка напряму зв'язана з так званим «центром задоволення». Саме пошук дофаміну (гормону задоволення) змушує людей будь-якого віку повертатись знову і знову до тих речей, які викликали його значне підвищення. Але у цієї ситуації є інша сторона: досліди показали [2], що у людей, які багато часу проводять перед екранами комп'ютера чи смартфону, спостерігались зміни в структурі тканин мозку. Це свідчить про передчасне старіння цієї області мозку. Окрім цього, підвищений рівень дофаміну в крові може викликати психічні та фізичні розлади, а саме стати причиною розвитку шизофренії, порушенню функціонування нирок та печінки.

Батьки повинні розуміти необхідність обмеження перебування їх дитини в мережі та області їх діяльності. Навіщо це потрібно:

– обмежити доступ дитини до небажаних матеріалів. Не вся інформація корисна та безпечна, деяка може навіть завдати психологічної травми або стати причиною небезпечних дій;

– контролювати переміщення дитини. Іноді діти можуть не виходити на зв'язок і саме тоді додатки для батьківського контролю допомагають впевнитись, що дитина саме там, де повинна бути і з нею все в порядку;

– задавати рамки годин доступу до пристрою. Навіть найбільш відповідальні діти можуть «загратися» і проводити більше часу за гаджетами, ніж дозволено;

– блокувати можливість придбання та встановлення додатків. Такий функціонал вбереже дітей від необачних витрат та обмежить доступ до непотрібного контенту;

– відстежувати активність дитини в соціальних мережах. Цей пункт не повинен виходити за етичні межі, але дає змогу відстежувати, на які сторінки дитина підписується, кого додає в друзі і з ким спілкується.

Часто самих повчальних бесід щодо небезпек в інтернеті мало і тоді варто звертатися до інших методів, як, наприклад, програмне забезпечення для батьківського контролю.

Зі свого боку ми намагаємось розробити мобільний додаток, який допоможе батькам зробити веб-серфінг для їх дитини абсолютно безпечним. На сьогодні найбільш популярним програмним забезпеченням є Qustodio [3] та NetNanny [4]. Саме із цих двох додатків ми виділили найкраще та взяли за ідею для нашого застосунку. Перед додатком поставлені наступні задачі:

– спростити моніторинг активності дитини в інтернеті та додатках (в соціальних мережах, як Facebook, Twitter, Instagram, WhatsApp, YouTube, посилання СМС та здійснення дзвінків, ігри);

– забезпечити якісну фільтрацію контенту, який буде «споживати» дитина;

– дати змогу батькам налаштувати розклад роботи пристрою;

– відстежувати місцеперебування членів сім'ї.

Таким чином, можна зробити висновок, що заходи щодо забезпечення безпеки дитячого перебування в мережі допоможуть не тільки вчасно виявити будь-які проблеми, але і м'яко їх вирішити. Адже далеко не всі діти діляться з батьками тим, що з ними відбувається, навіть якщо це може загрожувати життю та здоров'ю.

Список використаної літератури:

1. Діти інтернету – дослідження та статистика – Режим доступу до ресурсу: https://sites.google.com/site/kyrsbez/26-1

2. Комп'ютер та інтернет сповільнюють розвиток мозку дитини [Електронний ресурс] – Режим доступу до ресурсу: https://nauka.tass.ru/nauka/5892737

3. Qustodio [Електронний ресурс] – Режим доступу до ресурсу: https://www.qustodio.com/en/?source=aw&utm_source=awin&utm_medium=693909&utm_campaign=Webselenese+LTD&utm_term=Comparison+Engine&awc=7874_1618855449_8fa4ffc21f89e48d6c98774bc7b5a7ba&utm_content=text

4. Netnanny [Електронний ресурс] – Режим доступу до ресурсу: https://www.netnanny.com/products/?utm_source=cj&utm_medium=click&utm_campaign=publisher5302495&PID=10-5302495&cjevent=a66c1a41a13911eb8043025c0a180514.

МОБІЛЬНИЙ ДОДАТОК CARESSPET ДЛЯ ПОЛІПШЕННЯ СИТУАЦІЇ З БЕЗПРИТУЛЬНИМИ ТВАРИНАМИ

Журавель Н. Л.
Київський Національний університет технологій і дизайну
Марченко С. В.

Проблематика моніторингу та опіки над безпритульними тваринами особливо гостро стоїть у країнах східної Європи та СНД. Нині Україна входить в топ-10 країн світу, де найбільша кількість бродячих тварин, що вказує на недостатність зусиль та

малоефективність поточних підходів до вирішення цієї проблеми. У нашій країні вже існують проєкти, націлені на відстежування даної проблематики, зокрема Animal ID [1], Япомога [2] та ін. За їх даними, тільки в межах Києва нараховується понад 30000 бродячих собак.

Щодо ситуації в світі, то тільки в Індії нараховують близько 28 млн бродячих собак, у В'єтнамі – 7,2 млн, а в Камбоджі – 5 млн. Перенаселення безпритульними тваринами вже призводить до страшних наслідків [3]:

– збільшення кількості ДТП. Тварини переходять дорогу в неналежних місцях, що часто призводить до аварій з їх участю. Тільки в Індії кожного року помирає 25 млн безпритульних тварин через ДТП.

– укуси бродячих тварин. Кожного року в Індії близько 1,75 млн людей страждають від укусів бродячих тварин.

– сказ. Кожного року відбувається понад 20 тис. смертей людей через сказ. Це прямо пов'язано з понаднормовою популяцією безпритульних тварин, адже в 99% випадків, вірус сказу передається до людини саме через собак. Близько 90% смертей від сказу по всьому світу припадають саме на азійські країни.

– неетичні способи скорочення популяції. Присипляння, отруєння, вбивство за допомогою вогнепальної зброї – доволі «популярні» методи розв'язання проблеми перенаселення.

– погіршення роботи притулків. Волонтери не справляються з популяцією бродячих тварин, що змушує їх не дотримуватись звичайних правил утримування.

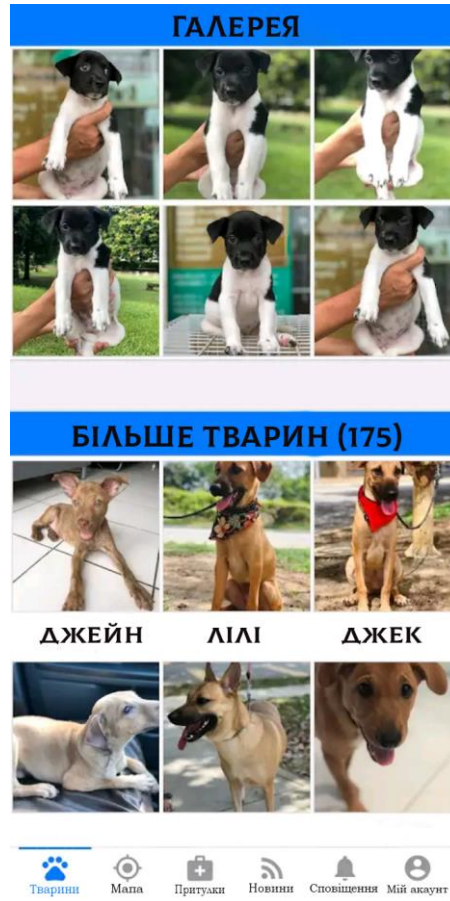
– торгівля собачим м'ясом. Тільки в Китаї щорічно вбивають понад 10 млн собак та 4 млн котів на продаж.

Різноманітні благодійні організації займаються цілим рядом дій [4]. Наприклад, в таких країнах як Туреччина, Великобританія, Румунія та ін. практикують вилов, подальшу стерилізацію тварин та їх повернення на минулі місця перебування. Зі свого боку, в Італії діє сценарій, який карає саме недбалих власників: у країні введено обов'язкову реєстрацію улюбленців, і якщо власник

позбавить тварину житла – його чекає великий штраф або навіть кримінальна відповідальність терміном до 3 років. Ще один дієвий метод – податок на утримання домашньої тварини. Він діє в таких країнах як Австрія, Норвегія та Франція. Власник тварини повинен не тільки зареєструвати улюбленця, але і заплатити податок, щоб підтвердити серйозність своїх намірів. А от Нідерланди – єдина країна, де не зареєстровано жодної бродячої тварини. Влада держави об'єднала всі найкращі підходи із міжнародної практики етичного відношення до тварин.

Зі свого боку ми намагаємось розробити мобільний додаток, який допоможе покращити доброустрій тварин шляхом облаштування прямої взаємодії зацікавлених сторін: тварин з притулків та їх майбутніх власників. Ідея PetFinder [5] – аналога додатку Tinder для знайомства користувачів з безпритульними собаками

та котами – була взята нами за основу. Його вигляд показано на рис. 1.



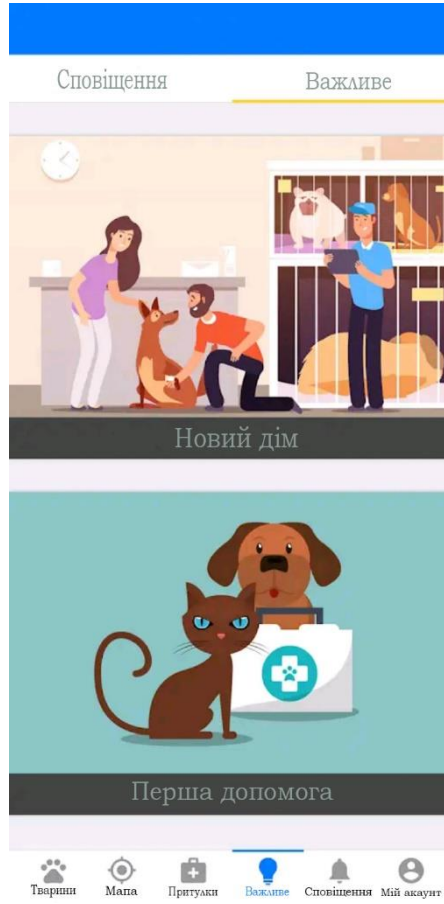


Рис. 1 Приклад роботи додатку

Перед додатком поставлені наступні задачі: зменшити кількість безпритульних тварин, шляхом знаходження їм нових власників; популяризувати допомогу бродячим тваринам серед різних шарів населення; допомогти власникам тварин знайти загублених улюбленців. Додаток буде корисний як волонтерам із притулків для тварин, так і потенційним власникам. У ньому можна знайти анкети потенційних домашніх улюбленців, їх розміщення на мапі та навіть поради щодо виховування та утримання тварин.

Таким чином, можна зробити висновок, що кожен із нас має змогу виправити складну ситуацію з безпритульними тваринами в нашій країні. Використовуючи досягнення в галузі інформаційних технологій, є можливість значно прискорити цей процес.

Література:

1. Animal ID [Електронний ресурс] – Режим доступу до ресурсу: https://animal-id.net/ru/site/about-project
2. Япомога [Електронний ресурс] – Режим доступу до ресурсу: https://yapomoga.com/cases/37
3. Consequences of Stray Dogs Overpopulation in Asia [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@adopsiorg/consequences-of-stray-dogs-overpopulation-in-asia-11e3c44d6e0c
4. Как разные страны решают проблему бездомных животных? [Електронний ресурс] – Режим доступу до ресурсу: https://34travel.me/post/city-animals
5. PetFinder [Електронний ресурс] – Режим доступу до ресурсу: [Електронний ресурс] – Режим доступу до ресурсу: https://www.petfinder.com/

GEOINFORMATION TECHNOLOGIES MODIS METHODS FOR ANALYZING THE DISTRIBUTION OF BLACK SEA PHYTOPLANKTON

Pervysheva Y.A.
National Aerospace University "Kharkov Aviation Institute"
Andrieiev S.M

Phytoplankton is the initial link in the food chain of the seas and oceans. The level of its development determines the productivity of the entire reservoir and the stocks of fish resources as well. Two-thirds of the oxygen on Earth is produced only by these single-celled planktonic algae. Therefore, phytoplankton are occasionally called as the "lungs of the planet". Though the presence of phytoplankton indicates sufficient nutrient conditions for phytoplankton to flourish, its high concentrations producing toxins build up results in

harmful algal blooms (HABs). The HABs, also known as red tides, primarily constitute blue-green algae or cyanobacteria. The cases of red tides have become more frequent in the recent decades and have attracted the close attention of the scientists around the world. The red tides or water blooming is considered one of the biggest contemporary problems since it has severe impacts on human health, aquatic ecosystems, and the economy as well.

In this regard, one of the tasks of environmental monitoring of the marines, carried out with the help of space technologies, is to monitor the development of these 'red tides' The MODIS Chlorophyll a layer provides the near-surface concentration of chlorophyll in milligrams of chlorophyll pigment per cubic meter (mg/m^3) in the ocean. Chlorophyll is a light harvesting pigment found in the photosynthetic organisms. All the phytoplankton in the ocean contain this green photosynthetic pigment. The marine phytoplankton capture almost an equal amount of carbon as land vegetation. Moreover, the change in phytoplankton number could result in the alteration of oceanic productivity. This provides an ocean link to global climate change modeling. The MODIS Chlorophyll a product is therefore a useful tool for assessing the health of the ocean.

According to satellite data, phytoplankton in the open water area of the Black Sea reaches its greatest development in the autumn-winter and winter-spring seasons, i.e. during the period of developed winter convection. This contradicts the ideas about the need for stable stratification for the development of winter-spring blooms in the waters of the temperate zone. The fact of rapid development of phytoplankton in the entire convective layer and the thickness of which in winter significantly exceeds the depth of the compensation point of photosynthesis. The coastal waters of Black sea are characterized by a pronounced peak in chlorophyll concentration associated with the rapid development of phytoplankton in March (flowering). In the open waters of the Black Sea, the spring peak of phytoplankton development in March is not observed according to averaged satellite data.

The reliability of the information in this research is extracted from the survey materials that depends to the greatest extent on several factors. The foremost of these

factors are the properties of the area of Black Sea being studied and the qualifications of the performer. Furthermore, the reliability of recognition of phytoplankton in the image is crucially determined by their spectral properties, the severity of the boundaries, the degree of variability, as well as the presence of stable relationships with other objects.

References

1. European Commission (EC) 2006. BS EN 15204: Water quality - Guidance standard on the enumeration of phytoplankton using inverted microscopy (Utermöhl technique): Brussels, 46 pp.

2. Jeffrey, S.W. and Humphrey, G.F. 1975. New Spectrophotometric equations for determining chlorophylls a, b, c1 and c2 in higher plants, algae, and natural phytoplankton. Biochem. Physiol. Planz., 167.

БАЗА ДАНИХ MINFORM ДЛЯ ВИКОРИСТАННЯ В СИНТЕЗІ ЦИФРОВИХ БЛОКІВ

Ямковий Артур Миколайович,
студент Київського національного університету технологій та дизайну
Бурмістров Сергій Владиславович

Актуальним питанням при розробці та проектуванні цифрових схем та синтезі цифрових блоків є етап, пов’язаний із спрощенням булевих функцій та отриманням мінімальної форми вказаної булевої функції. Даний процес є досить трудомістким та протяжним у часі.

Досвід проектних робіт при розробці цифрових пристроїв вказує на те, що практично в навчальній діяльності основна маса булевих функцій, що використовується,– це булеві функції від двох, трьох або чотирьох аргументів. Саме вказані функції становлять основу ядер блоків цифрових схем досліджуваних пристроїв.

Метою проекту є створення нового способу синтезу цифрових блоків, який полягає в заміні етапу мінімізації булевих функцій використанням каталогів уже

готових результатів мінімальних форм булевих функцій. З метою реалізації нового способу синтезу потрібно побудувати відповідну впорядковану за номерами базу даних мінімальних форм функцій, а саме розробити комплексну ієрархічну базу даних мінімальних форм з повним набором результатів в базисі класичної логіки (AND, OR, NOT) та в базисі алгебри Жегалкіна (AND, XOR, «1»). Структура каталогу зумовлена особливостями будови булевих функцій та їхніми характеристиками.

Ієрархічна структура бази даних є оптимальною з точки зору економії загального об'єму бази та з точки зору запобігання дублювання даних. Суть ієрархії полягає в тому, що кожному елементу таблиці вищого рівня прикріплено таблицю нижчого рівня.

Структура бази даних складається з таблиць, які охоплюють БФ по вказаним критеріям:

- таблиці даних за кількістю аргументів, по вазі коду в таблиці істинності, ;
- таблиці даних змісту мега-групи релятивності, змісту груп релятивності;
- таблиці розв'язків булевих функцій в класичній формі представлення;
- таблиці коефіцієнтів складності реалізації булевих функцій в класичній формі представлення;
- таблиці розв'язків булевих функцій в алгебрі Жегалкіна та в формі Рідда-Мюллера;
- таблиці принципових логічних схем в класичній формі представлення, в алгебрі Жегалкіна;
- таблиці даних коефіцієнтів складності реалізації в алгебрі Жегалкіна.

Вказана структура дає можливість швидко знаходити потрібні дані та максимально зменшити об'єм використовуваної пам'яті базою даних. На основі бази даних планується побудувати ряд запитів та відповідних форм звітів з метою професійного користування інформацією вказаної бази даних.

Зміст бази даних планується сформувати за допомогою програмного середовища Borland Delphi 7.0. В середовищі планується створити потрібну статистичну інформацію для каталогу з врахуванням того, що будь-яка функція може бути задана в двійковому, десятковому та шістнадцятковому коді.

Практичним результатом даного проекту є база даних, яку планується використати в навчальному процесі з метою зменшення витрат часу студентами на побудову готових пристроїв.

Література:

1. Чебурахин И. Ф., Гавриш О. Н. Об эффективных методах синтеза булевых формул и схем из функциональных элементов. Мехатроника, автоматизация, управление. Том: 18. Выпуск: 6. Стр. 407-414.

ПЕРСПЕКТИВНА СУЧАСНА ПЛАТФОРМА ДЛЯ РОЗРОБКИ ІГОР

Кобякова Є. С.
ISMA University of Applied Science, Latvia
Хотунов В. І.

Анотація

Феномен відеоігор це новий і дуже актуальний напрям для наукових досліджень, що минув шлях за дуже малий термін в декілька десятиліть від малих і локальних робіт в різних сферах науки, таких як маркетинг, культурологія, філософія і т. п. до великих наукових досліджень з безліччю варіантів вивчення такого цікавого об'єкта дослідження, як відеоігри. Мета даної роботи - проаналізувати ринок і тенденції розвитку відеоігор, визначити найбільш перспективний напрямок для невеликих IT-компаній.

Вступ

На сьогоднішній день світова індустрія відеоігор є одним із значних частин глобальної економіки, а самі ігри давно стали сприйматися багатьма користувачами

як якісна багатогранна розвага, яка знаходить велику популярність серед населення світу. Так само сфера відеоігор в сучасному світі є дуже високооплачуваною нішею.

Відеоігри сильно вплинули так само і на інші сфери мистецтва і розваг. Існує величезна кількість сайтів, журналів, теле-передач, які присвячені темі відеоігор, знімається велика кількість фільмів, в основі яких лежать сюжети відеоігор (наприклад, Lara Croft, World of Warcraft, Mortal Combat, Resident Evil і інші).

Так само варто згадати феномен «гейміфікація», коли ігрові практики використовують в неігрових сферах (в основному в рекламній, освітній, військовій і т.п.), що несе в собі цілі залучити й утримати більшу аудиторію, сприяє допомозі в навчанні.

Відеоігри сильно вплинули на соціальну складову. Багато жанрів включають в себе «мультикористувацький режим», коли користувачі можуть не тільки підключатися до однієї ігрової сесії, а й активно спілкуватися через текстові чати і голосові технології безпосередньо під час гри.

За останні сім років ринок відеоігор виріс на 60% в порівнянні з іншими сферами розваги. У рік в середньому ринок досягає до 160 мільярдів доларів, впевнено обганяючи кіноіндустрію. Половина обсягу ринку відеоігор знаходиться в Азіатському регіоні (Китай, Корея, Японія), наступну позицію займає Північна Америка (близько 30%) і Західна Європа (близько 20%). Головним фактором розвитку ринку відеоігор є розвиток інтернет-технологій і здешевлення интернет-послуг, а також доступність до техніки (комп'ютерів, смартфонів) для користувачів і спрощення розробки самих відеоігор.

Огляд

З огляду на величезну різноманітність відеоігрових платформ, метою даної роботи є дослідження найбільш відповідної платформи для відкриття команди розробників в невеликій IT компанії.

Для прийняття рішення будуть розглянуті такі критерії:

• Поточне положення на ринку відеоігор

• Співвідношення середнього часу, що витрачається користувачами.

• Модель поширення і окупність

• Складність розробки

В даний час користувачі віддають перевагу мобільному геймінгу, що включає в себе ігрові програми на планшетах і смартфонах, що можна пояснити зручністю і доступністю таких додатків, а також легкістю в освоєнні ігор за такою технологією. Цей сегмент займає 36% ринку відеоігрової індустрії, а серед усього ринку мобільних додатків 80%. Популяризація цифрових ігрових магазинів і мобільних додатків дозволили спростити процес видання мобільних ігор для невеликих студій. Розробники, які створюють ігри в малих командах без підтримки офіційних видавців як правило створюють «інді-ігри» (так звані «незалежні відеоігри»). Подібні ігри не мають обмеження, дозволяють виявити «творчу свободу», але і не відрізняються великим масштабом. Завдяки популярності інді-ігор часто у малі студії розробки інвестують великі видавці, не обмежуючи при цьому їх творчі ідеї. Вибравши мобільну платформу можна спростити модель поширення і забезпечити окупність гри.

Висновок

Виходячи з дослідження, можна зробити висновок, що найкращим вибором для невеликого відділення розробників ігор в наш час стане вибір мобільної платформи завдяки простоті розробки, її популярності і спроможності укласти вигідний договір з компанією-видавцем.

Література:

[1] Chen J. Flow in Games (and Everything Else) // Communications of the ACM, 2019, no. 50 (4), c. 31–34

[2]Ветушинський А. Для проведення ігрових досліджень натисніть кнопку СТАРТ // Логотипи. 2018. №1 (103). С. 41–60.

[3] Богост Дж. Розлад у відеоіграх // Логотипи. 2018. No 1 (103). С. 79–99.

[4] Девід В. Ласкаво просимо до Pong-Story: Сайт першої відеоігри - http://www.pong-story.com/intro.html.

МОЖЛИВОСТІ ВИКОРИСТАННЯ ДОДАТКА SLACK ДЛЯ ВИРІШЕННЯ ПРОБЛЕМИ ВНУТРІШНЬО-КОРПОРАТИВНИХ КОМУНІКАЦІЙ

Мараховський Д. С.
denysmarakhovskyi@gmail.com
Маріупольський державний університет
к.п.н., доцент Ротаньова Н. Ю.

Відомо, що обмін інформацією є одним із найскладніших та універсальних процесів, з якими доводиться стикатися більшості компаній. Розмаїття мобільних додатків та веб-сервісів, котрі застосовують для внутрішньо-корпоративних комунікацій, з одного боку, сприяє покращенню комунікаційних процесів та способів виконання інструкцій; з іншого боку, призводить до наступних проблем:

- хаотичного спілкування, розділеного між електронною поштою, чатами, дзвінками тощо, й відсутності доступу до історії спілкування для всіх зацікавлених сторін;

- зростання потоків інформації та її безсистемного впорядкування, оскільки необхідні матеріали часто розкидані між відділами, проектними групами, пристроями тощо;

- нераціонального використання часу при надсиланні й отриманні електронних листів, текстових повідомлень та дзвінків.

- відсутності уніфікованої системи для перевірки роботи працівника й оцінювання її продуктивності.

З метою вирішення означених вище проблем вважаємо за доцільне вивчити можливості використання додатка Slack, котрий слугує для забезпечення внутрішньої системи зв'язку. Розробниками вказано наступні переваги Slack [3]: створення простору для спільної роботи, спілкування та обміну файлами завдяки тому, що чат організовано за каналами й це дозволяє працівникам спілкуватися

миттєво та прозоро; окрім того, всі зацікавлені сторони мають доступ до інформації без зайвого перевантаження поштової скриньки.

Аналіз наукових праць свідчить про ефективність додатка Slack для організації співпраці між представниками структурних підрозділів компаній, дослідницькими групами тощо й високий рівень задоволеності цим інструментом серед працівників, дослідників та студентів. Ученими М. Гофін та С. Кларк представлено модель інтеграції комунікаційних технологій в дослідницьку діяльність епідеміологів, котрі потребують ефективного спілкування в режимі реального часу та спільного доступу до численних документів для ефективного управління дослідженням. Автори зазначають, що Slack легко інтегрується в робочий процес у міському академічному медичному центрі й сприймається користувачами як високоефективний інструмент для задоволення потреб комунікації між дослідницькими групами та впорядкування спільних документів. Slack, котрий має як настільні, так і мобільні версії, архівує всі прямі повідомлення та групові розмови, розміщує та впорядковує документи, інтегруючись з додатком Google Docs [1].

Цінними є результати дослідження А. Тухкали та Т. Керккяйнена, котрі вивчали процес комп'ютерно-опосередкованого спілкування за допомогою Slack у закладах вищої освіти. Зокрема, вчені розглядали можливість використання Slack для організації взаємодії студентів під час роботи над магістерським дослідженням. Результати опитування показали, що студенти сприймали Slack як простий у використанні інструмент спілкування й виявили бажання послуговуватися ним у майбутньому, проте стикалися з проблемами, пов'язаними з управлінням файлами та аутентифікацією користувачів [4].

Учені акцентують, що безкоштовна версія Slack дозволяє інтегрувати не менше десяти інших додатків, зокрема Trello, Google Drive, Google Hangouts Simple Poll, Skype тощо, що є важливим, наприклад, при проведенні конференцій. Водночас, обробка інформації великою кількістю сервісів може призвести до

плутанини й суттєво зменшити значущість інструменту Slack, який призначено для посилення продуктивності спілкування та збереження інформації в одному місці [2, с. 151].

Підсумовуючи сказане вище, доцільно відзначити, що, незважаючи на зручність та інтеграційні можливості додатку Slack, необхідним є розроблення методичних рекомендацій для учасників ділової або навчальної комунікації щодо особливостей його використання.

Література:

1. Gofine M., Clark S. Integration of Slack, a cloud-based team collaboration application, into research coordination: a research letter. *Journal of Innovation in Health Informatics.* 2017. № 24. P. 252-254.

2. Johnson H. A. Slack. *Journal of the Medical Library Association.* 2018. № 106. P. 148-151.

3. Slack makes it downright pleasant to work together : веб-сайт. URL: https://slack.com/intl/en-ua/

4. Tuhkala A., Kärkkäinen T. Using Slack for computer-mediated communication to support higher education students' peer interactions during Master's thesis seminar. *Education and Information Technologies*. 2018. № 23. P. 2379-2397.

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ЗА ДОПОМОГОЮ СУЧАСНИХ СОЦІАЛЬНИХ МЕРЕЖ

Семичасний Ярослав Миколайович
здобувач вищої освіти 2 курсу факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ
Кисельов Андрій Олександрович
доцент кафедри оперативно-розшукової

діяльності факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
майор поліції

Сучасні системи інформаційної безпеки передбачають використання відеоспостереження. Здійснюється відеофіксація того, що відбувається в місцях загального доступу: в аеропортах, вокзалах, на стадіонах, та ін. Використання зображень, отриманих за допомогою систем відеоспостереження забезпечує виконання функцій охорони громадського порядку, безпеки дорожнього руху, захисту власності тощо.

Для належного функціонування суспільства, поліція має повноваження затримувати, тимчасово утримувати під вартою і допитувати осіб, підозрюваних у вчиненні кримінальних правопорушень, та інших категорій осіб, визначених законодавством [1]. Утім, здійсненню цих повноважень внутрішньо притаманні ризики залякування затриманих та фізичної наруги над ними. Затримані особи перебувають під владою держави, що автоматично накладає на співробітників поліції відповідальність створення безпечних умов тримання цих людей [2].

Держава також зобов'язана врахувати усі загрози та небезпеки, які потенційно можуть виникнути щодо затриманих осіб, як з боку персоналу або інших посадових осіб держави, так і з боку інших затриманих .

Водночас слід відмітити, що такий розподіл було нами зроблено не із врахування кількості чи якості отриманої первинної оперативно-розшукової інформації, а саме за періодичністю здійснення таких заходів працівниками кримінальної поліції в повсякденній роботі.

Разом із цим аналіз сучасної кримінальної обстановки, способу життя населення, використання все частіше злочинним елементом електронних способів зв’язку дає змогу дійти висновку, що необґрунтовано мало використовуваними є

способи, пов'язані з аналізом та моніторингом як інтернет-ресурсів, так і соціальних мереж чи інших електронних платформ спілкування населення [3].

Зокрема, не для кого не є сьогодні новим, що саме за допомогою інтернет-ресурсів, електронних менеджерів і створених на їх основі каналів, чатів, співтовариств тощо відбувається розповсюдження наркотичних засобів, психотропних речовин та їх аналогів [4].

Так, Т.О. Чистанов зазначає, що класичний спосіб збуту наркотичних засобів сьогодні здійснюється шляхом залишення їх у схованках, так званих «закладках», що має на увазі організацію безконтактного збуту, коли координація діями й обмін інформацією співучасниками, а також із замовником здійснюється за допомогою телекомунікаційних мереж і мобільних додатків, таких як Facebook. З причини складної ситуації у сфері незаконного обігу наркотичних засобів необхідно вживати заходів щодо контролю за діяльністю інтернет-сервісів у сфері телекомунікацій (Facebook і т.д.).

У всьому світі розробники мобільних додатків у сфері телекомунікацій слідують сучасним тенденціям захисту переданої інформації, збереження приватності й неможливості потрапляння інформації в публічний доступ. Правоохоронні органи не мають можливості відслідковувати координаційні вказівки організаторів незаконного обороту, у свою чергу це ускладнює отримання інформації, яка на стадії попереднього і судового слідства могла б стати ключовим доказом причетності осіб до злочинної діяльності. Наприклад, розробники месенджера WhatsApp використовують технологію наскрізного шифрування, яка не дозволяє нікому іншому, включно з організацією Facebook, прочитати надіслані повідомлення. Ще більш потужні алгоритми захисту інформації використовуються в месенджері Facebook.

Таким чином, інформація, передана між співучасниками незаконного обігу наркотиків, надійно захищена і недоступна для правоохоронних органів.

Список використаної літератури:

1. Чистанов Т.О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств. URL: https://research-journal.org/law/nezakonnyj-sbyt-narkoticheskix-sredstv-s-ispolzovaniemtelekommunikacionnyx-setej-i-ustrojstv/.

2. Баб'як А.В. Отримання та використання первинної оперативно-розшукової інформації оперативними підрозділами ОВС України : монографія. Львів : Каменяр, 2010. 167 с.

3. Активисты поймали педофила. URL: https://www.facebook.com/watch/?v=1757294501243980.

4. В Украине нашли три десятка угнанных в Италии мотоциклов. URL: https://ua.korrespondent.net/ukraine/4003209-v-ukraini-znaishly-try-desiatky-vykradenykh-v-italiimototsykliv.

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ ЗА ДОПОМОГОЮ СУЧАСНИХ СОЦІАЛЬНИХ МЕРЕЖ

Лозовий Олександр Андрійович
здобувач вищої освіти 2 курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ
Кисельов Андрій Олександрович
доцент кафедри оперативно-розшукової
діяльності факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
майор поліції

Останнім часом соціальні мережі відіграють все більше значення у подіях, котрі розгортаються у реальному світі. Рівень розвиненості і охоплення соціальних мереж, дозволяє нам використовувати їх з несподіваних сторін. Форуми та месенджери – стають одним із інструментів демократії, саме ними користувалися протестувальники у Гонконгу для прийняття консолідованих рішень.

Проблематикою і питанням інституалізації соціальних мереж науковці займаються з початку минулого століття. Спершу питання мережевої структури суспільства було сферою інтересів соціологів, філософів та математиків, однак із винайдення мережі Інтернет і появи перших соціальних мереж науковці почали активно досліджувати потенціал та ризики, котрі несуть із собою сучасні технології, у вигляді соціальних мереж. В останні роки активізувалися дослідження ролі соціальних мереж на політичну стабільність державних інституцій та вплив мереж на здоров'я людей. Таким чином, науковці роблять акцент на негативних аспектах розвитку соціальних мереж, лишаючи поза увагою потенційні вигоди від них для суспільства. В наступних частинах роботи спробуємо розглянути тенденції комунікаційних стратегій та тактик, якими оперують користувачі в різних ситуаціях соціальної нестабільності та напруження [1].

Викладене не охоплює всіх проблемних аспектів створення та розвитку кримінального аналізу в національному правовому полі, однак дає підстави для здійснення подальших наукових розробок [2]. Варто також погодитись із висновками вчених, які вважають, що дослідження засад кримінального аналізу як позитивного досвіду застосування аналітичних інструментів у сфері протидії кіберзлочинності країнах Євросоюзу доцільно покласти в основу розробки теоретико-методологічних засад його прикладного використання в національну кіберпросторі.

Успішна реалізація та впровадження нових методів кримінального аналізу дасть можливість у майбутньому поширити її на всю систему Національної поліції України та активно використовувати аналітичні способи і прийоми, завдяки яким

можливо забезпечити виконання завдань оперативно- розшукової діяльності, створить передумови для більш ефективного виконання суб'єктами оперативно-розшукової діяльності своїх завдань і правоохоронних функцій, що, своєю чергою, сприятиме підвищенню ефективності протидії кіберзлочинності [1].

При активному розвитку кримінального аналізу за кордоном слід підкреслити неналежне вітчизняне наукове визначення даного поняття. Зокрема, Інтерполом було прийнято таке визначення терміна «кримінальний аналіз» – ідентифікація та забезпечення спостереження взаємозв'язків між даними щодо злочинів та іншими відомостями, потенційно пов'язаними зі злочинами, у практичній діяльності поліції та судових органів з метою надання допомоги особами, які приймають рішення щодо протидії злочинності, у подоланні невизначеності, а також забезпечення вчасного відвернення загроз й аналітична підтримка оперативної діяльності [3].

Відзначимо, що слабкість систем Instagram та частково систем варто в бідності і поверхні методів аналізу; системи закриті; системи не в повній мірі враховують специфіку соціальних мереж, не володіють можливістю збору даних і обробляють відносно малі їх обсяги.

Виходячи з аналізу достоїнств і недоліків систем, як висновок можна зробити наступний висновок: ідеальна система аналізу соціальних мереж повинна: працювати на всіх рівнях аналізу (від моніторингу соціальних мереж до прогнозу і управління) в різних режимах (в режимі реального часу і ретроспективному режимі), аналізувати різні об'єкти соціальної мережі (від окремо взятого інформаційного повідомлення і окремо взятого користувача до соціальної мережі в цілому і зовнішніх по відношенню до неї джерел) і враховувати різні відношення між такими об'єктами (зв'язку знайомств між пользова- ками, зв'язку цитування , зв'язку коментування та ін.), базуватися на математичних моделях і методах інтелектуальні аналізу даних (статистичних і графових), інтегруватися з підсистемами збору даних з різних відкритих джерел (соціальних мереж, блогових

платформ, новинних ресурсів і т.д.), обробляти дуже великі масиви даних (терабайти даних, мільйони вузлів мережі і сотні мільйонів зв'язків між ними) [2].

Крім того, важливо, щоб така система була орієнтована на «звичайного» аналітика в певній предметній області. Видається очевидним, що розробка серйозної системи інтелектуального аналізу соціальних мереж (Instagram) для всіх можливих користувачів вельми складна і економічно не точна (схожість по функціональності сучасних систем різного призначення пояснюється тим, що вони знаходяться тільки на початку свого розвитку). Тому можна припустити, що в найближчі роки з'являться системи для конкретних кінцевих користувачів, які вирішують приватні завдання в тих чи інших предметних областях.

Література:

1. Кримінальне право України. Загальна частина : [підручник] / [Ю.В. Баулін, В.І. Борисов, Л.М. Кривоченко та ін.] ; за ред. проф. В.В. Сташиса, В.Я. Тація. – К. : Юрінком Інтер, 2007. – 496 с.
2. Бізнес ФОП: торгівля в Інстаграмі. URL : https://journal.ostapp.com.ua/uk/articles/post/biznes-flp- torgovla-v-instagrame (дата звернення: 07.05.2020).
3. Багрій М., Луцик В. Деякі проблеми законодавчого регулювання проведення негласних слідчих (розшукових) дій. Право України. 2017. No 12. С. 39–48.

СУЧАСНІ МЕТОДИ МАСШТАБУВАННЯ ПІКСЕЛЬНИХ ЗОБРАЖЕНЬ

Горобинський А. С.
gorobinskiya5@gmail.com
Київський національний університет технологій та дизайну
Марченко С. В.

Сучасний стандарт роздільної здатності в кінематографі та комп’ютерній графіці – 4К – передбачає близько чотирьох мільйонів пікселів для отриманих цифрових зображень. Разом з тим, користувачу пропонуються відеоматеріали і зразки комп’ютерної графіки відповідно до стандартів 1080p, 720p, 480p та навіть

ще гіршої якості. Це призводить до значних спотворень зображення на сучасних екранах, появи артефактів і розмитості. Очевидно, що з часом дана тенденція буде тільки посилюватись, оскільки вже з'являються телевізори з підтримкою стандарту 8К (мінімум 33 мільйони активних пікселів). Звідси, в сучасних реаліях особливої актуальності набувають алгоритми масштабування зображень, тобто підходи до їх цифрової обробки, що мають на меті зміну роздільної здатності зі збереженням пропорцій та якості. Зауважимо, що масштабування працює в обидві сторони: алгоритми апскейлінгу (upscaling – збільшення розміру) та даунскейлінгу (downscaling – зменшення роздільної здатності). З проблемою масштабування стикаються найрізноманітніші компанії, особливо хмарні сервіси, яким необхідно зберігати терабайти цифрових зображень та оптимально управляти сховищами даних. Важливими галузями діяльності також є реставрація старих кінокартин чи іншої відеопродукції, ремастеринг ігрових проектів тощо [1].

За останнє десятиліття значно змінились підходи до масштабування зображень. Від початкових ідей щодо застосування чисельної інтерполяції значень пікселів і до впровадження машинного навчання для покращення якості зображень пройдено тривалий еволюційний шлях. Нині популярні такі алгоритми масштабування піксельних зображень [2]:

– інтерполяція методом найближчого сусіда. Один з найпростіших методів збільшення розміру зображень, який заміняє кожний піксель на декілька пікселів того ж кольору. Зображення стають більшими, проте мають значну кількість артефактів та проблеми зі збереженням гладких контурів об'єктів;
– білінійна інтерполяція. Двовимірна лінійна інтерполяція, має непогані результати, проте масштабовані зображення отримуються з небажаним пом'якшенням (розмиттям) об'єктів на них;
– бікубічна інтерполяція. Покращена інтерполяція, до якої також відносять фільтри Ланцоша та Мітчелла-Нетравалі;

– інтерполяція на основі перетворень Фур'є. Тригонометрична інтерполяція, яка аналізує частотну область зображення. Характеризується хорошим збереженням деталей на зображенні, проте може вносити кільцеві артефакти (ringing artifacts);
– інтерполяція вздовж контурів деталей (Edge-directed interpolation). Алгоритми концентруються на збереженні контурів зображення після масштабування. До цієї категорії відносять методи New Edge-Directed Interpolation (NEDI), Edge-Guided Image Interpolation (EGGI), Iterative Curvature-Based Interpolation (ICBI), Directional Cubic Convolution Interpolation (DCCI);
– векторизація зображень. Спочатку створюється векторне, незалежне від роздільної здатності представлення растрового зображення. Після цього відбувається масштабування та зворотна растеризація зображення. Цю методику використовують такі програмні продукти, як Adobe Illustrator, Inkscape та ін;
– методи на основі навчання згорткових нейронних мереж. Нині це панівні підходи, пов'язані з застосуванням машинного навчання для масштабування зображень. Нейронні мережі можуть тренувати на розпізнавання деталей зображення та заповнення новоутворених при збільшенні зображення пікселів відповідно до розпізнаного шаблону.

Чільне місце в даному контексті посідає вимірювання якості зображення. Оцінка ефективності та якості результатів масштабованих цифрових зображень дозволяє здійснювати порівняння різних алгоритмів за цими критеріями та відбір найбільш доречних з них у конкретних умовах. Серед метрик якості зображень при масштабуванні часто використовують пікове відношення сигналу до шуму (Peak Signal-to-Noise Ratio, PSNR), індекс структурної подібності (SSIM, Structural Similarity), середню оцінку думки (Mean Opinion Score), якість сприйняття на основі навчання (Learning-based Perceptual Quality) та ін. [3].

Список використаних джерел

1. What Is AI Upscaling? [Електронний ресурс] – Режим доступу до ресурсу: https://blogs.nvidia.com/blog/2020/02/03/what-is-ai-upscaling/#:~:text=Basic%20upscaling%20is%20the%20simplest,of%20the%20higher%20resolution%20display.
2. Comparison gallery of image scaling algorithms [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://wiki2.org/en/Comparison_gallery_of_image_scaling_algorithms.
3. Wang Z. Deep Learning for Image Super-resolution: A Survey / Z. Wang, J. Chen, S. C. Hoi. // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2020. – doi: 10.1109/TPAMI.2020.2982166.

Секція 4.

Сучасні напрямки розвитку

веб-технологій

ОГЛЯД ДОСТУПНИХ РІШЕНЬ ПРИ МОДЕЛЮВАННІ АЛГОРИТМУ ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Баландін Кирило Євгенович
Феночка Роман Віталійович
Відокремлений структурний підрозділ «Фаховий коледж інженерії та управління Національного авіаційного університету»,
Апенько Н.В., к.т.н.
Київ, Україна

Система розпізнавання облич – це технологія, здатна ідентифікувати або перевірити особу на цифровому зображенні або відеокадрі. Існує багато методів, які використовуються в системах розпізнавання осіб, але в цілому вони ґрунтуються на порівнянні рис обличчя заданого зображенням з обличчями, які зберігаються в базі даних. Він також описується як біометричний додаток на основі штучного інтелекту, який може однозначно ідентифікувати людину шляхом аналізу моделей на основі текстур обличчя та форми людини[1].

Спочатку системи розпізнавання облич застосовувалось як застосунки, останнім часом все частіше використовуються на мобільних платформах та в інших технологіях, таких як робототехніка. Зазвичай він використовується для контролю доступу в системах безпеки нарівні з іншими біометричними системами, такими як розпізнавання райдужної оболонки, відбитки пальців[2]. Хоча точність системи розпізнавання облич як біометричної технології є нижчою, ніж розпізнавання райдужної оболонки ока та розпізнавання відбитків пальців, вона широко застосовується завдяки безконтактному та неінвазивному процесу[3]. Останнім часом вона також стала популярною як комерційний інструмент ідентифікації та маркетинговий інструмент. Інші застосунки мають такі елементи, як просунута взаємодія людини з комп'ютером, відеоспостереження, автоматичне індексування зображень та відео[4].

OpenCV. OpenCV (Open-Source Computer Vision Library) – це бібліотека з відкритим кодом, що пропонує алгоритми комп'ютерного зору та машинного

навчання. Вона розроблялась з 1999 року, і нараховує більш ніж 47 000 членів спільноти. Це сама велика керована спільнотою бібліотека для комп'ютерного зору та алгоритмів машинного навчання. OpenCV написана на C ++ і пропонує інтерфейси на Python, C ++, Java і MATLAB. Бібліотека пропонує понад 2500 алгоритмів і тому є найбільшим доступним рішенням щодо комп'ютерного зору та машинного навчання. Будь то державні органи або корпорації, такі як Google або Microsoft, всі вони користуються цією бібліотекою, що робить її доступною бібліотекою для комп'ютерного зору та машинного навчання. OpenCV був спеціально розроблений для програм у реальному часі, тобто розпізнавання облич за допомогою камери для отримання миттєвого зворотного зв'язку потоку камери.

OpenFace. OpenFace – це бібліотека розпізнавання облич, що використовує глибокі згорткові нейронні мережі для розпізнавання облич. Вона використовує нейронний мережевий підхід на основі систем Google Facenet. Вона містить нейронну мережу, що пройшла навчання з 500 тис. зображень. Розпізнавання можна здійснити, надавши зображення точки доступу Python і викликаючи способи виявлення обличчя плюс попередню обробку на даному зображенні. OpenFace потім додасть його до нейронної мережі, таким чином зробивши розпізнавання простим у реалізації.

OpenBR. OpenBR – це платформа з відкритим вихідним кодом, запущена в 2013 році. Вона заснована на OpenCV для своїх алгоритмів і використовує фреймворк Qt для крос-платформної сумісності. Структура спеціально розроблена для швидкого прототипу алгоритмів і здатна забезпечити зрілу фреймворк. Окрім основних рамок, OpenBR пропонує плагіни, такі як HOG, PCA та інші, які можна додати, якщо потрібно.

По оцінкам компанії MarketsandMarkets в найближчі роки ринок відеоаналітики продовжить активно рости, а до 2020 складе 3971 мільйонів доларів. Даний напрямок активно розвивається. Одною із задач, які вирішує відеоаналітика,

є розпізнавання облич у відеопотоках. Рішення даної задачі в першу чергу має безпосереднє застосування в системах контроля доступу і ідентифікації особистості.

Задача розпізнавання облич має серйозну практичну перспективу, так як цей метод ідентифікації особистості для людини є природнім і реалізовується на інтуїтивному рівні. З точки зору обману системи сучасні методи ідентифікації по обличчю поки програють в надійності в порівнянні з ідентифікацією по райдужній оболонці ока, але рахується надійніших, ніж розпізнавання по відбиткам пальців чи геометрії зап'ястя. Традиційні системи ідентифікації потребуються знання пароля, наявність ключа, ідентифікаційної карточки, чи іншого ідентифікаційного предмета, який можна забути чи згубити. На відміну від них, біометричні системи засновуються на унікальних біометричних характеристиках людини, які важко підробити і які однозначно визначать конкретну людину. До таких характеристик відносяться відбитки пальців, форма долоні, райдужна оболонка, зображення сітчатки ока, індивідуальні характеристики обличчя.

Eigenfaces – алгоритм, запропонований в 1991 році Метью Терком і Алексом Пентланд [2], який здобув широку популярність в якості першого успішного методу розпізнавання осіб. Основною ідеєю алгоритму є застосування методу головних компонент для знаходження векторів, найкращим чином описують зображення осіб. Використовуючи цей метод можна виявити різні зміни в навчальній вибірці зображень облич і описати цю зміну в базисі декількох ортогональних векторів, які називаються власними (eigenface). Обличчя, мають корисну властивість: зображення, яке відповідає кожному вектору має форму обличчя. Обчислення головних компонент зводиться до обчисленню власних векторів і власних значень коваріантної матриці, яка розраховується із зображення.

Fisherfaces – алгоритм, в якому на відміну від методу eigenfaces використовується лінійний дискримінантний аналіз, а саме лінійний дискримінант Фішера. Дія алгоритму заснована на пошуку проекції даних, при якій класи

зображень облич максимально роздільні. При використанні методу головних компонент проводиться максимізація розкиду даних по всій базі облич.

Будь-який з алгоритмів Eigenface або Fisherface виявляє вимоги до розпізнавання облич має свої переваги та недоліки. Тому дані алгоритми в даний час використовуються спільно один з одним в залежності від потреб проекту. Дослідження доступних відкритих рішень показало, що OpenCV є основою розпізнавання облич, яка розроблялася протягом тривалого часу, тоді як OpenFace і OpenBR є досить новими. Пізніші рішення також вирішують різні проблеми розпізнавання облич. OpenBR, наприклад, інтенсивно розробляється для швидкого прототипування алгоритмів, тоді як OpenFace намагається більше використовувати інший нейромережевий підхід. OpenFace і OpenBR також є нестандартними рішеннями, тому пропонують значно менше досвіду навчання при реалізації проекту. OpenCV також спеціально розроблений для реальних додатків. Проект спрямований на використання приладу в режимі реального часу через потік камери, що робить цю функцію основним функціоналом, необхідним для роботи проекту. Дослідження Delbiaggio на тестах алгоритму розпізнавання облич показує, що OpenFace та LBPH мають найвищу точність розпізнавання на тестовому наборі з 5 різних осіб з 40 зображеннями кожен, з Eigenface і Fisherface з нижчою точністю.

Література:

1. OpenCV [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – URL: https://uk.wikipedia.org/wiki/OpenCV.

2. Розпізнавання облич [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – URL: http://uk.wikipedia.org/wiki/Розпізнавання_облич.

3. Модулі email та smtplib[Електронний ресурс] // Сайт «python–scripts». – URL: https://python–scripts.com/send–email–smtp–python

4. Ознаки Хаара [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – URL: https://uk.wikipedia.org/wiki/Признаки_хаара.

ВИЩА ОСВІТА ЯК АКТУАЛЬНИЙ НАПРЯМОК РОЗВИТКУ ВЕБ-ТЕХНОЛОГІЙ В УКРАЇНІ

Крулевський А.В.,
a.krulevskyi@gmail.com, магістр
Західноукраїнський національний університет

Темп розвитку сучасного світу зумовлює до постійних змін та удосконалень у різноманітних сферах суспільного життя та економіки. Людина, у свою чергу, шукає шляхи оптимізації свого часу та інформації, яка сприймається нею. Беручи до уваги вищевказане, можемо зазначити, що вища освіта є доволі актуальним та перспективним напрямком для розвитку веб-технологій в Україні. Вища освіта є майданчиком з широким колом можливостей зокрема, для оптимізації доступних знань та формування інтерактивних методів навчання. Передумовами для розвитку веб-технологій в освіті є постійне зростання кількості населення, яке охоплене інтернет-технологіями та активне використання молоддю сучасних технологій особливо, використання мобільних пристроїв.

На даний момент є багато різноманітних веб-технологій, які вже використовуються у різних сферах життєдіяльності людини зокрема, технології, які на даний момент використовуються в інших країнах та є новими для України і технології, які є новими для інших країн та поки що недоступними для України через економічну та політичну нестабільність. Проте, беручи до уваги розвиток України та освіти зокрема, варто відзначити наступні веб-технології, які є доступними та перспективними для розвитку у вищій освіті в Україні, а саме:

- хмарні технології - є популярною технологією, яка використовується у різних сферах та активно удосконалюється. Використання та розвиток хмарних технологій у вищій освіті в Україні дозволить забезпечити доступ до інформації незалежно від місцеположення та надасть можливість модернізувати процес навчання і розширити географію студентів навчального закладу. Крім цього,

дозволять розробити ефективну систему для роботи між студентами та викладачами у міжнародному форматі [1].

- дистанційне навчання та мобільні технології – необхідність ефективного використання часу зумовлює розвиток дистанційного навчання та мобільних технологій. Можливість навчатись дистанційно і при цьому, використовувати мобільні технології є елементом зручності оскільки, студент зможе ефективно використовувати свій час, навчаючись у найбільш відповідний для себе період, а також навчатись «на ходу» за допомогою мобільних технологій [2,3].

- віртуальна та доповнена реальність - це технології, які є популярними на цей час проте, ще недостатньо розвинені та мають безліч напрямків для удосконалення. Розвиток цих технологій у вищій освіті в Україні дозволить студентам активно освоювати практичні процеси, які важко відтворити у реальному світі або через певні чинники, які не дозволяють повною мірою дослідити певне питання. Крім того, вищевказані технології нададуть можливість урізноманітнити навчальний процес з метою збільшення зацікавленості студентів та ефективнішого засвоєння інформації [3].

- віртуальні робочі середовища - зазначена технологія дозволить проводити різноманітні експерименти, які недоступні у реальності, використовуючи необмежене місцеположення та можливості міжнародної співпраці. Доволі ефективним буде використання із віртуальною та доповненою реальністю [2,4].

Розвиток цих технологій також, потребує створення ефективної комплексної системи оскільки, маючи цілісну систему, можна забезпечити ефективну роботу цих технологій для того, щоб вивести вищу освіту в Україні на новий рівень, шляхом забезпечення студентів актуальною, цікавою та доступною інформацію з інтерактивним процесом навчання.

Впровадження та активний розвиток сучасних веб-технологій у вищій освіті дозволить значно підвищити економічний потенціал України оскільки, дозволить підготовлювати сучасних, висококваліфікованих спеціалістів, які зможуть

ефективно пристосовуватися до ринкових умов та зробити значний внесок у розвиток економіки України. Крім цього, дозволить отримувати фінансування від вітчизняних та іноземних інвесторів. Для цього не менш важливим є активне сприяння та підтримка зі сторони держави оскільки, тільки спільними зусиллями можливо створити ефективну систему для розвитку сучасних веб-технологій у вищій освіті в Україні та сприяти постійному удосконаленню.

Література:

1. Вакалюк Т.А. Можливості використання хмарних технологій в освіті. *Інформаційно-комунікаційні технології в освіті: мат. доп. Міжнар. наук.-практ. конф.*(м. Острог, 1-2 листопада 2013 року). Херсон, 2013. С. 97-99. URL: http://eprints.zu.edu.ua/10137/1/%D0%92%D0%B0%D0%BA%D0%B0%D0%BB%D1%8E%D0%BA%20%D0%A2.%D0%90..pdf)

2. Demianenko V., N. Ichanska. Використання сучасних веб-технологій для системи контролю та моніторингу знань. *Збірник наукових праць «Системи управління, навігації та зв'язку».* Полтава: ПНТУ, 2019. Т. 2 (54). С. 83-86. URL: http://journals.nupp.edu.ua/sunz/article/view/1413/1205

3. Тищенко М. А. Деякі аспекти використання сучасних освітніх інформаційно-комунікаційних та веб-технологій у вищих начальних закладах України. *Міжнародний мультидисциплінарний науковий журнал «ЛОГОΣ. Онлайн», Педагогічні науки.* Вінниця, 2019. № 3. URL: https://www.ukrlogos.in.ua/10.11232-2663-4139.03.04.html

4. Дутчак М., Лазарович І., Яновський Ю., Web 3.0 - технології в інтелектуальних освітніх онлайн-платформах. *Proceedings of the 2019 Scientific Seminar on Innovative Solutions in Software Engineering*.(м. Івано-Франківськ, 10 грудня 2019 р.). Івано-Франківськ, 2019. С. 7-9. URL: http://lib.pnu.edu.ua:8080/bitstream/123456789/8318/1/7_dutchak_lazarovych_yanovskyi.pdf

ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ САЙТОБУДУВАННЯ

Семенюк Р.М.,
semlana81@gmail.com
Хмельницький університет
управління та права
ім. Леоніда Юзькова
Фасолько Т.М., к.е.н., доцент

Початок XXI століття характеризується швидким розвитком науки і техніки. Це пов'язано зі значним прискоренням науково-технічного прогресу в результаті науково-технічної революції, що почалася в середині XX століття.

Тенденцією сучасного будівництва сайтів є поява так званого глибокого або невидимого веба. Вперше термін "глибокий веб" було введено Джиллом Іллсвортом у 1994 році, для характеристики ресурсів, які з тих чи інших причин не доступні звичайним пошуковим системам. Під невидимим вебом слід розуміти текстові, аудіовізуальні документи, веб-сторінки та цілі веб-сайти, на які в Інтернеті немає посилань.

З перших днів існування Інтернету відбулося поступове, а потім прискорене проникнення у всі сфери людської діяльності (наука, освіта, виробництво, соціальні справи та комунікації тощо).

З появою Інтернету та розвитком його послуг розпочався перехід на електронні форми традиційних документів: стрічки новин на інформаційних сайтах, особисті перевірки в блогах, журналах, що публікуються на різних веб-сайтах. Крім того, така послуга, як відеохостинг, пропонує традиційне телебачення. З'являються нові види мистецтва, такі як цифровий живопис, електронна музика, комп'ютерна анімація тощо.

Слід зазначити, що переваги Інтернету як засобу масової інформації та веб-сайтів в цілому та подання документованої інформації дозволили їм зайняти провідне місце в сучасному інформаційному суспільстві серед засобів документування, зберігання та обробки інформації, що поступово зменшує частку документів з паперовими носіями інформації. Це можливо завдяки постійному

розвитку як самої мережі Інтернет (зменшення вартості доступу до Інтернету для кінцевих користувачів, зниження витрат та поліпшення якості провайдерів роумінгу, збільшення швидкості передачі даних тощо), так й інструментів документування та представлення інформації на веб-сайтах в Інтернеті, поява нових технологій управління цими веб-сайтами, призначених для полегшення взаємодії з користувачами.

При цьому веб-сайт повинен не тільки містити стандартний набір інформації про компанію, товари чи послуги, але також повинен забезпечувати ефективний зв'язок між її підрозділами, замовниками та постачальниками. У той же час, уможливлюється суттєве зменшення витрат на первісні вкладення (для створення веб-сайту чи веб-сторінки).

Наступні фактори сприяють популярності Інтернету, а також розвитку та розповсюдженню технологій створення веб-сайтів як способу представлення інформації, задокументованої в цій мережі:

– доступність Інтернету як способу документування, обміну, зберігання та використання інформації;

– різноманітність інструментів документації, в тому числі безкоштовних, для зберігання, обміну та використання інформації та для їх швидкого подальшого розвитку;

- можливість отримати доступ до інформації, яка вже задокументована в Інтернеті, або опублікувати задокументовану інформацію в цій мережі з будь-якої точки світу, де є підключення до мережі Інтернет, практично з будь-якого мобільного пристрою;

- перерозподіл світового ринку праці на основі організації роботи з віддаленими працівниками, які не працюють у штаб-квартирі компанії і можуть знаходитися в інших населених пунктах, країнах та континентах.

Все це дозволяє прогнозувати зростання популярності мережевих технологій та служб Інтернету. Про це свідчать, наприклад, дослідження міжнародної

аналітичної компанії IDC, що були здійснені на замовлення американської компанії EMC Corporation.

Сучасні тенденції розвитку технологій для створення та управління веб-сайтами включають:

– використання технологій обробки інформації, що виконуються користувачами, таких як JavaScript, Flash, Silverlight тощо;

– розробка та розвиток концепції Web 2.0 як засобу спрощення інформаційної документації;

– захист вмісту веб-сайту як інтелектуальної власності від несанкціонованого використання: копіювання, друку, надсилання тощо;

– існування "глибокої мережі", тобто сайту EIR, до якого не пов'язаний жоден інший сайт EIR.

Проаналізувавши тенденції та перспективи розвитку сайтобудування можна зробити висновок, що переваги веб сайтів займають лідируючи позиції у сучасному інформаційному суспільстві та є надзвичайно важливими для суспільства у XXI столітті.

Список використаних джерел:

1. Перелік типових документів, що створюються під час діяльності органів державної влади та місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів : наказ Міністерства юстиції України від 12.04.2012 № 578/5 : зареєстровано в Міністерстві юстиції України 17.04.2012 за № 571/20884 // Офіц. вісн. України. К., 2012. № 34. Ст. 1272.
2. Тенденції та перспективи розвитку сайтобудування, їх вплив на архівне копіювання веб-сайтів / Т.Я. Купрунець // Архіви України. 2013. № 6. С. 95-104. Бібліогр.: 17 назв. укр.
3. Теорія розробки Веб-сайту [Електронний ресурс] - Режим доступу : URL : http://pidruchniki.com/2015082665983/informatika/teoriya_rozrobki_veb-saytu

SINGLE PAGE APPLICATIONS

Коваль О. В., firnenwind@gmail.com
Київський національний університет технологій та дизайну
Чепинога А. В.
м. Черкаси, Україна

На сьогоднішній день цифрова індустрія є надзвичайно популярною, конкурентною та стрімко розвивається. Все більше і більше сфер нашого життя з кожним днем діджиталізуються та приймають вигляд веб-сервісів та мобільних додатків.

Найбільш ефективний підхід розвитку в таких умовах – клієнтоорієнтованість. А невеликий об'єм уваги клієнтів, що стрімко скорочується ще сильніше спонукає компанії до пошуку нових кращих способів забезпечення швидкої безперебійної роботи своїх сервісів.

Це стало причиною через яку багато компаній стали розробляти частини своїх веб-додатків з використанням нового веб-дизайну – Single Page Application. Два найбільш масштабних на сьогоднішній день сервіси – Google і Facebook також використовують цей підхід.

Для того, щоб розуміти що привносить SPA дизайн важливо знати за яким принципом працюють MPA – Multi Page Applications. Багатосторінковий додаток – це класичний веб-додаток, в якому кожного разу, як відбувається обмін даними сервер надсилає нову сторінку для відображення на стороні клієнта. Об'єм контенту, що передається величезний, і через це, як правило, такі додатки багаторівневі та зі значною кількістю посилань.

В свою чергу SPA додаток – це в прямому сенсі одна сторінка, яка постійно взаємодіючи з користувачем динамічно змінює поточну сторінку замість того, щоб завантажувати цілі сторінки з серверу. Прикладами односторінкових додатків є система моніторингу задач Trello, соціальні мережі Facebook та Twitter, система електронної пошти Gmail.

Основою роботи односторінкових додатків є те, що завантажується та змінюється лише частина елементів. Ті ж елементи, які не потребують змін не будуть навантажувати трафік та систему.

Головні переваги SPA підходу:

- Швидкість роботи. Так як немає необхідності оновлювати всю сторінку, а лише ті елементи, що були змінені, такий підхід позитивно впливає на швидкість роботи додатку.

- Висока швидкість розробки. Готові бібліотеки та фреймворки дають потужні інструменти для розробки веб-додатків. Над додатком можуть одночасно працювати як back-end так і front-end розробники, так як завдяки чіткому розділенню вони не будуть заважати один одному.

- Мобільні додатки. SPA підхід дозволяє легко розробити мобільний додаток на основі існуючого коду, він дозволяє використовувати вже існуючий back-end майже без змін.

Але односторінкові додатки також мають свої недоліки:

- Погана SEO оптимізація. Особливості роботи SPA додатків унеможливлюють сканування більшості сторінок пошуковими ботами. Через це просування сайту в пошукових системах може бути ускладненим.

- Неактивний javascript. Деякі користувачі відключають javascript у своїх браузерах, що робить неможливим роботу сайту, так як він використовує javascript для оновлення даних.

- Низький рівень безпеки.

SPA дизайн добре підходить для розробки динамічних платформ з невеликим об’ємом даних. Також аргументом на користь такого підходу стане необхідність в майбутньому розробити мобільний додаток для розроблюваного сервісу. Цей дизайн добре підходить для таких типів проектів як SaaS платформи, соціальні мережі, закриті співтовариства. Для створення великих інтернет магазинів, бізнес сайтів, каталогів, маркетплейсів, де велику роль грає SEO оптимізація та немає

необхідності створювати мобільний додаток ліпшим рішенням буде використовувати класичний MPA підхід.

Література:

1. Single page application (SPA) и multi page application (MPA): преимущества и недостатки. URL: https://merehead.com/ru/blog/single-page-application-vs-multi-page-application/

2. Что такое SPA-приложения. URL: https://wezom.com.ua/blog/chto-takoe-spa-prilozheniya

РОЗРОБКА СЕРВЕРНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОДАТКІВ

Лисенко Д.О., drovk199995@gmail.com
Київський національний університет технологій та дизайну
Хотунов В.І.
м. Черкаси, Україна

Одним з шляхів розвитку сучасних веб-технологій є створення програмного системного забезпечення (далі – ПЗ), яке виконує значну кількість функцій від авторизації до обробки мільйонів запитів за хвилину.

На даний момент розробка серверного програмного забезпечення є одним з головних стовпів при розробці додатків, що оперують з різними даними.

Серверне ПЗ дозволяє обробляти, зберігати, кешувати, аналізувати велику кількість інформації, що відкриває горизонти для використання машинного навчання разом с серверним ПЗ.

При створенні більшості додатків потребується веб-сервер, який буде отримувати запити від додатку та обробляти їх та повертати відповідь, яка може бути в будь-якому форматі: від HTML сторінки до файлу, архіву. Для розробки серверного ПЗ використовують різні мови програмування. Їх обирають в залежності від складності, задачі, швидкості роботи бажаного додатку.

На даний момент серверне програмне забезпечення стало ще більше охочим за популяризації хмарних технологій, які привнесли нові можливості для розробки.

Хмарні технології дозволили з легкістю налаштовувати веб-сервери, масштабувати їх та використовувати їх не тільки для прийому запитів и віддавання відповіді, а й для обробки великих даних, запуску самостійних команд в визначений час, що будуть виконувати різні функції і т.д.

Серверне програмне забезпечення для додатків створене API та сервіси, з якими спілкується мобільний додаток для того, щоб отримувати нову інформацію та зберігати або оновлювати інформацію, яку надсилає користувач, цю частину називають backend.

Цей підхід покращує розробку, пришвидшує процес планування задач, також він дозволяє розділити зобов'язана між людьми, які займаються проектуванням архітектури та роботи додатку. Також такий підхід полегшує тестування продукту на різних стадіях його розробки. API забезпечує взаємодію між двома системами. Це як гвинтик, що зв'язує дві деталі, або як шестерня, за допомогою якої наводяться в рух дві сусідні шестерінки.

В кінцевому рахунку, розробники викликають API незримо для користувача для добування інформації в свої додатки. Кнопка в графічному інтерфейсі користувача програмно підключена для виклику зовнішніх служб. Наприклад, кнопки Twitter або Facebook, які взаємодіють з соціальними мережами, або відео Youtube, які витягують відео з ресурсу youtube.com, працюють під управлінням веб-API.

Розробка серверного ПЗ розвивається дуже швидко зараз через те, що з кожним днем системи стають все складніші, архітектура змінюється, кількості запитів збільшуються через все більше використання Інтернету та збільшення варіацій хмарних технологій, які розробляють різні компанії гіганти, щоб покращувати стабільність та швидкість роботи серверів.

ФРЕЙМВОРКИ ДЛЯ РОЗРОБКИ ВЕБ-ОРІЄНТОВАНИХ ДОДАТКІВ, ЇХ ПЕРЕВАГИ ТА НЕДОЛІКИ.

Оношко О.В.
Київський національний університет технологій та дизайну
Хотунов В.І.
м. Черкаси, Україна

Швидкість, з якою поширюється інформація сьогодні, є вражаючою. Інтернет став каталізатором до поширення інформації. Інтернет майорить сайтами різноманітного спрямування від розважальних до навчальних. Розвиток Інтернету прямо пропорційно пов'язаний з розвитком та проектуванням сайтів. Масове використання сайтів зумовлює гостру проблему, а саме питання щодо якості цих самих сайтів. Популярність створення веб-ресурсів сприяла розробці різних систем і програм, які спрощують процес розробки сайту. Вони допомагають підвищити ефективність роботи, а також дозволяють розробнику сфокусуватися над основною логікою програми. Такі технології, як PHP, Java, Microsoft.Net, MySQL, Oracle, Microsoft SQL Server і розроблені на їх основі фреймворки – це каркаси системи або під системи, що можуть включати допоміжні програми, мови сценаріїв, і все, що має на меті полегшити розробку й дає змогу об'єднати різні компоненти.

Програмний фреймворк – це готовий до використання комплекс програмних рішень, включаючи дизайн, логіку та базову функціональність системи або підсистеми. Відповідно – програмний фреймворк може містити в собі також допоміжні програми, деякі бібліотеки коду, скрипти та загалом все, що полегшує створення та поєднання різних компонентів великого програмного забезпечення чи швидке створення готового і не обов'язково об'ємного програмного продукту. Побудова кінцевого продукту відбувається, зазвичай, на базі єдиного API.

В сучасному сайтобудуванні використання фреймворків набуває популярності Це зумовлено тим, що розробка за допомогою фреймворку зменшує навантаження на процес розробки веб-додатків. Такий результат досягається тим, що розробка з використанням фреймворку позбавляє від проблеми використання

повторюваного коду. Використання фреймворків робить процес створення програми більш легким і функціональним. На сьогоднішній день існує сотні фреймворків для створення веб-додатків. Це в свою чергу ускладнює вибір фреймворку, так як кожен з них має велику кількість привабливих функцій та доповнень. Необхідно враховувати, що неправильний вибір фреймворку може стати ключовою причиною провалу проекту.

Переваги використання фреймворків:

- гнучкість і масштабування – завжди має гнучке рішення нестандартних завдань і можливість далі розширення функціоналу шляхом підключення сторонніх бібліотек або окремих класів; ефективне використання ресурсів сервера;

- використання підходу MVC суттєво розширює функціонування та гнучкість проекту, так як використовується під час проектування та розробки програмного забезпечення. Фреймворки написані розробниками для розробників, що дозволяє мати на виході прекрасно написаний код і своєчасне виправлення помилок;

- наявність детальної документації з використання фреймворку;

- безпека – забираються всі проломи в безпеці, практично немає вузьких місць для SQL-ін'єкцій; фреймворк дозволяє сконцентруватися на вирішенні архітектурних завдань, а не базових, як при розробці без його застосування;

- якість матеріалу на виході.

Недоліки застосування фреймворку досить умовні і незначні порівняно з перевагами:

- важко обслуговувати – якщо проект створював один розробник, а потім з якихось причин він пропадає або просто відмовляється супроводжувати створений ним проект, то його подальший розвиток і обслуговування стає більш складним питанням і часто не вигідним заняттям;

- ціна розробки – вартість стандартного сайту зробленого з використанням фреймворку з нуля буде дорожче, ніж на CMS, тому що часу на розробку

витрачатися в кілька разів більше. Багато коду не використовується і лежить мертвим вантажем в проекті;

- складність в освоєнні.

Література:

1. Аналіз фреймворків як засобів розробки web-додатків [Електронний ресурс] – Режим доступу до ресурсу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DB=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/mnj_2016_6(1)__23.pdf

2. Анализ шести веб-фреймворков: плюсы, минусы и особенности выбора [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/ruvds/blog/343894/.

ТРАСУВАННЯ ПРОМЕНІВ В РЕАЛЬНОМУ ЧАСІ

Кошовий Андрій Олегович
Черкаський державний бізнес-коледж
Ратайчук П.Є
м. Черкаси, Україна

Трасування променів (англ. Ray tracing; рейтрейсінг) - один з методів геометричної оптики – дослідження оптичних систем шляхом відстеження взаємодії окремих променів з поверхнями. У вузькому сенсі – тех.нологія побудови зображення тривимірних моделей в комп'ютерних програмах, при яких відстежується зворотна траєкторія поширення променя (від екрану до джерела).

Трасування променів в комп'ютерних іграх – це рішення для створення реалістичного освітлення, відображень і тіней, що забезпечує більш високий рівень реалізму в порівнянні з традиційними способами рендеринга. Turing стала першою архітектурою, що дозволяє проводити трасування променів в реальному часі на GPU.

Компанія Nvidia представила технологію RTX. Як ми і припускали, це технологія трасування променів в реальному часі. Як стверджує Nvidia, RTX є

плодом десятирічної роботи компанії. Лише зараз графічні прискорювачі стали настільки продуктивними, щоб зробити трасування променів в реальному часі доступною для використання в іграх.

Nvidia RTX – платформа, яка містить ряд корисних інструментів для розробників, які відкривають доступ до нового рівня комп'ютерної графіки. Nvidia RTX доступна тільки для нового покоління відеокарт Nvidia GeForce RTX, побудованого на архітектурі Turing. Основна особливість платформи – наявність можливості трасування променів в реальному часі (також званої рейтресінгом).

Трасування променів – функція, яка дозволяє імітувати поведінку світла, створюючи правдоподібне освітлення. Зараз в іграх промені рухаються не в реальному часі, через що картинка, найчастіше, хоч і виглядає красиво, але все одно недостатньо реалістична - використовувані зараз технології вимагали б величезна кількість ресурсів для рейтресінгу.

Це виправляє нова серія відеокарт Nvidia GeForce RTX, що володіє достатньою потужністю для розрахунку шляху променів.

Переваги:

- можливість рендерингу гладких об'єктів без апроксимації їх полігональними поверхнями (наприклад, трикутниками);
- обчислювальна складність методу слабо залежить від складності сцени;
- висока алгоритмічне розпаралелюваність обчислень - можна паралельно і незалежно трасувати два і більше променів, розділяти ділянки (зони екрану) для трасування на різних вузлах кластера тощо;
- відсікання невидимих поверхонь, перспектива і коректне зміни поля зору є логічним наслідком алгоритму.

Недоліки:

Серйозним недоліком методу зворотного трасування є продуктивність. Метод растеризації і сканування рядків використовує когерентність даних, щоб

розподілити обчислення між пікселями. У той час як метод трасування променів кожен раз починає процес визначення кольору пікселя заново, розглядаючи кожен промінь спостереження окремо. Втім, цей поділ тягне поява деяких інших переваг, таких як можливість трассіровать більше променів, ніж передбачалося для усунення контурних нерівностей в певних місцях моделі. Також це регулює відображення променів і ефекти заломлення, і в цілому - ступінь фотореалістичності зображення.

RTX проектує промені світла з точки зору гравця (камери) на навколишній простір і вираховує таким чином, де якого кольору піксель повинен з'явитися. Коли промені натикаються на що-небудь, вони можуть:

Відбитися - це спровокує появу відображення на поверхні;

Зупинитися - це створить тінь з того боку об'єкта, на яку світло не потрапив

Переломити - це змінить напрямок променя або вплине на колір.

Наявність цих функцій дозволяє створювати більш правдоподібне освітлення і реалістичну графіку. Цей процес – дуже ресурсозатратне і давно застосовується при створенні ефектів фільмів. Різниця лише в тому, що при рендер кадру фільму у авторів – доступ до великого обсягу ресурсів і, можна вважати, необмеженому проміжку часу. В іграх же на формування картинки у пристрої є частки секунди і відеокарта використовується, найчастіше, одна, а не кілька, як при обробці кінокартин.

Це спонукало Nvidia впровадити додаткові ядра в відеокарти GeForce RTX, які візьмуть на себе більшу частину навантаження, покращуючи продуктивність. Вони також забезпечені штучним інтелектом, завдання якого - вираховувати можливі помилки під час процесу трасування, що допоможе їх уникнути заздалегідь. Це, як заявляють розробники, також підвищить швидкість роботи.

Під час презентації відеокарт Nvidia продемонструвала ряд прикладів роботи трасування променів: зокрема, стало відомо, що деякі майбутні ігри, включаючи Shadow of the Tomb Raider і Battlefield 5 будуть працювати на платформі RTX. Функція ця, проте, буде в грі необов'язковою, так як для трасування потрібна одна з

нових відеокарт. Трейлери, показані компанією під час презентації, можна побачити нижче:

Як заявляла Nvidia під час своєї презентації, освоєння технології RTX дозволить значно поліпшити графічну складову ігор, розширюючи доступний розробникам набір інструментів. Проте, поки рано говорити про загальну революції графіки - дану технологію будуть підтримувати не всі ігри, а вартість відеокарт з її підтримкою досить висока. Презентація нових відеокарт значить, що прогрес в графічних деталях є, і з часом він буде все рости і рости.

Використана література

1. ТРАССИРОВКА ЛУЧЕЙ И ТЕХНОЛОГИЯ DLSS [Електронний ресурс] – Режим доступу до ресурсу: https://www.nvidia.com/ru-ru/geforce/rtx/.

2. Революція в графіці [Електронний ресурс] – Режим доступу до ресурсу: https://kanobu.ru/articles/revolyutsiya-vgrafike-chto-takoe-trassirovka-luchej-372475/.

ОСОБИСТИЙ БРЕНД ЗА ДОПОМОГОЮ ВЕБ-ТЕХНОЛОГІЙ

Антошик А.М.,
alinantoshyk@gmail.com
ЛНУ ім. Івана Франка
Калиняк Н.Є.

В епоху розвитку сучасних інформаційних технологій, все більше працедавців при прийнятті на роботу стали звертати увагу на такий аспект, як особистий бренд кандидата. Проте, який зв'язок між ІТ-сферою та особистим брендом? Відповідь доволі проста. Особистий бренд в XXI столітті формується, як правило, за допомогою веб-технологій. Це соціальні мережі, сайти, веб-додатки тощо. І головне, що ця тенденція набирає стрімких обертів.

Під поняттям «особистий бренд» ми повинні розуміти унікальність [1]. Чим краще кандидат вміє оперувати своїми навичками та досвідом, тим більше йому довіряють, тим більш конкурентоспроможною є компанія, в якій він працює. І, як

результат, залучення більшої кількості прихильників та споживачів у дану компанію.

Важливою умовою формування особистої стратегії є створення успішного бренду [2]. Адже успішність приводить до довіри з боку інших людей. Оскільки, в більшості випадків, транслювання особистості відбувається через соціальні мережі, то варто розуміти, що саме дозволяється висвітлювати особі.

В 90% випадків при заповненні резюме необхідно вказати посилання на соціальні мережі. Це робиться не тільки з метою подальшої комунікації, але й для того, щоб до моменту співбесіди спеціалісти з набору персоналу могли частково вивчити та переглянути життя кандидата. Але не завжди те, що вони бачать в профілі може відповідати реальності, це так званий синдром «дистанційної упередженості» [3]. Термін означає ситуацію, коли висновки про людину робляться лише на основі її власного подання себе, ігноруючи обставини реального життя. Таке спостерігається за користувачами Facebook, Instagram та Tik-Tok. Адже користувачі завжди є життєрадісними і не показують жодного негативу. Тому дуже важливим моментом є ведення сторінки так, щоб вона відображала людину такою, яка вона є. Оскільки невідповідність може зменшити шанси працевлаштування, а інколи й взагалі сильно відобразитися на кар'єрі спеціаліста.

Сучасне використання веб-технологій дає зрозуміти наскільки нетипово можна застосовувати інформаційні технології. Зокрема, створення резюме у вигляді сайту. Реалізується даний спосіб через написання HTML-коду у відповідних програмах, наприклад Visual Studio Code. Макети розробляти можна у редакторі Figma. Зрозуміло, що чим привабливішим та зрозумілішим буде резюме, тим більше шансів успішне на працевлаштування.

Існує низка переваг при використанні веб-резюме:

1. Не такий, як усі. Тобто можливість виділитися з-поміж інших кандидатів своєю відкритістю до нового.

2. Більше шансів бути заміченим. Оскільки, це новий спосіб подання себе, то компанії одразу будуть виділяти такі кандидатури в першу чергу.
3. Використання новітніх технологій. Це означає, що особа слідкує за тенденціями в розвитку ІТ-сфери і їй цікаво реалізовувати всі зміни на практиці.
4. Економія часу. Створений сайт дозволяє не розміщувати резюме на десятках сайтів, а навпаки кожен охочий роботодавець може сам ознайомитися із потенційним кандидатом.

Таким чином, використання такого веб-резюме дозволить збільшити об'єм інформації про людину. Крім цього, веб-сторінки індексуються більшістю пошукових систем та інтернет-каталогами, що підвищує шанси перегляду веб-резюме роботодавцями. А також на відміну від звичайних резюме, розміщених на сайтах з пошуку роботи, які видаляються через певні проміжки часу, веб-резюме не втрачають своєї актуальності упродовж тривалого часу. Проте, це не означає, що такого роду резюме не можна використовувати на сайтах з пошуку роботи. Зробити це можна, просто залишивши посилання на персональну сторінку.

Література:

1. Божук С.Г., Колотвина Е.Н., Тэор Т.Р. Бренд-менеджмент: учеб. пособие. Санкт-Петербург: СПбГИЭУ, 2011. 82 с.
2. Балабанова Л.В., Холод В.В. Маркетингове управління конкурентоспроможністю підприємств: монографія. Донецьк: ДонДУЕТ ім. М. Туган-Барановського, 2006. 294 с.
3. Соцмережі поглинають час і щастя їхніх користувачів? *Ukrainian news*: веб-сайт. URL: https://ukrainian.voanews.com/a/facebook-02-22-2012-140010953/247703.html (дата звернення 19.04.2021).

USE OF SCRUM METHODOLOGY IN IT PROJECTS

Lukianenko D.V.,
lukianenko1305@gmail.com
Cherkassy State Business College
Grygorash O.A.

«Simplicity – the art of maximizing the amount of work not done – is essential.»[3]

(C) Agile Manifesto

Scrum is the backbone of the process that includes a set of methods and predefined roles. This is a useful tool to finish a lot of things, as it keeps the teams focused on immediate priorities by breaking a huge project into small chunks. At each next stage, Scrum issues a working version of the final product (the simplest working product - MVP). This allows the team to improve the project gradually, rather than trying to do it from the beginning.

Many people associate Scrum sprints with Agile software development so often that Scrum and Agile are synonymous. However, this is not the case. Agile is a set of principles, and Scrum is a technique for active problem solving. The numerous similarities between globally agile and scrum processes make the two concepts related.[5]

Scrum Methodology Concept

Agile, Scrum project management has three fundamental parts:[1]

- Roles
- Practices
- Documents (artifacts)

Most often a scrum team consists of about 7 people. Each team has:

• participants (developers, designers);

• product owner who understands the market and the user, formulates tasks in the language of business and users, invents and selects tasks for product development;

• scrum master (scrum evangelist) who trains the members of the Scrum Team to interact with each other and with business representatives, as well as optimizes processes, increasing their efficiency.

There are users and stakeholders around the team and the owner of the product who asks these people for advice.

Sprint is an integral part of the activities. Sprint is a period of time of about a week, less or more, during which a "ready", i.e. usable and released incremental product is created. The effective development requires sprints of the same length.

During the sprint:[2]

• no changes are allowed that could jeopardize the goal of the sprint;

• product quality should not be reduced;

• the scope of work can be improved and re-agreed between the Product Owner and the Development Team.

Each sprint is an experiment. Its results must be verified and adapted. If it cannot be done, the sprint is considered a failure.

Retrospective

It is important to ask the right questions. The questions are much more constant than the answers. Retrospective is an opportunity to evaluate and analyze the work done. Retro covers a very wide range of specific goals that should be aligned with the top-level goal: to take steps to improve the process and improve team performance.

On the one hand, each case particular may require a special retro format. On the other hand, all good retrospectives have a certain set of attributes that allow them to run as productively as possible.

Overview

The retrospectives as What was good / What can be improved / Action items; Start / Stop / Continue; are based on the analysis of how to continue to do what works and change or get rid of what does not work. Such retros are sufficiently general and universal to allow them to be used in virtually any context in a non-standard way.

Root Cause Analysis

Root Cause Analysis can be grouped separately using Ishikawa Diagram and 5 Why's It works well for resolving recurring problems and allows you to focus on addressing the root cause, but not the symptoms.

Canvas

The various canvases serve well to create a comprehensive but short summary for further analysis. They can be used to construct a conceptual dashboard to structure key information. The constant repetition of retrospectives makes them ineffective, so there are now many interesting sites / applications which make the retrospective unique.

Specialized books are a huge source of information for a scrum master, business analyst, project manager and for all who want to optimize their time and resources and become more productive. Among the mostly recommended are "Brilliant agile"[7] and "The strongest."[6]

Scrum helps to get into the "flow" - the state of the highest concentration, when you do what you need to do, and not expending efforts, not forcing yourself and not pushing. [4]The main thing for successful work is to achieve and manage this state.

Scrum philosophy is simple and scrum principles are reasonable. Moving to the real application of scrum is a big challenge for each team. It is necessary not only to learn a new approach to project management, but also to find people who can work in scrum mode.

Literature:

1. Henrik Kniberg. Scrum and XP: notes with advanced = Scrum and XP from the trenches. - C4Media, 2007. - p. 140.
2. Mike Cohn. Scrum: Flexible Development = Succeeding with Agile: Software Development Using Scrum. - M .: «Williams», 2011. - p. 576
3. Jeff Sutherland. SCRUM. Revolutionary project management method = SCRUM. The art of doing twice the work in half the time. - Mann, Ivanov and Ferber, 2016. - p. 288

4. Kenneth Rubin. Essential Scrum: A Practical Guide to the Most Popular Agile Process. - M .: «Williams», 2016. - p. 544.
5. What is scrum? : веб-сайт. URL: https://www.digite.com/agile/scrum-methodology/ (дата звернення: 15.04.2021).
6. Сильнейшие. Бизнес по правилам Netflix: веб-сайт. URL: https://www.yakaboo.ua/sil-nejshie-biznes-po-pravilam-netflix-1907495.html (дата звернення: 15.04.2021).
7. Блистательный Agile. Гибкое управление проектами с помощью Agile, Scrum и Kanban : веб-сайт. URL: https://kniga.biz.ua/book-blistatelnyi-gibkoe-upravlenie-proektami-s-pomoshchiu-i-0024984.html (дата звернення: 15.04.2021).

ETHERCHANEL ТА ПІДВИЩЕННЯ НАДІЙНОСТІ МЕРЕЖІ

Брусенцов В.В.,
Київський національний університет технологій та дизайну
Чепинога А.В.
Черкаси, Україна

З початку винайдення комп'ютерних технологій прогрес стрімко виріс за останній час. І з кожним роком, потребує швидшу та надійнішу мережу в корпораціях. Для цих цілей була винайдена технологія Etherchanel, або ж її називають агрегацією фізичних каналів. Дана технологія, дозволяє об'єднувати декілька фізичних каналів в один логічний. Таке об'єднання дає можливість підвищити пропускну здатність та надійність каналу. Агрегацію каналів можна настроїти між двома комутаторами, комутатором та маршрутизатором, між комутатором та сервером. Агрегація каналу дозволяє вирішить такі задачі наприклад:

- підвищити пропускну здатність;.
- забезпечити резерв на випадок виходу з ладу одного з каналів.

Etherchanel дозволяє використовувати всі інтерфейси одночасно. При цьому пристрої контролюють поширення широкомовних фреймів щоб вони не зациклювались. Для цього комутатор, при отриманні широкомовного кадру через звичайний інтерфейс, відправляє його в агрегований канал тільки через один інтерфейс. А при отриманні, не відправляє його назад.

Ця технологія не є ідеальною. Вона підвищує пропускну здатність, але не бажано розраховувати на балансування навантаження між інтерфейсів в агрегованому каналі. Технологія балансуванню навантаження орієнтовані як правило на такі критерії:

- MAC-адресам
- IP - адресам
- портам відправників то отримувачів

Тобто завантаженість конкретного інтерфейсу ніяк не враховується. Тому що один інтерфейс може бути більш завантаженим ніж інші. Більш того, при неправильному виборі методу балансування або в деяких топологіях, може скластися ситуація коли будуть передаватися через один інтерфейс.

Для агрегації каналів в Cisco може бути використане один із трьох варіантів:

- LACP (Link Aggregation Control Protocol)
- PagP (Port Aggregation Protocol)
- Статичне агрегування без використання протоколів

Так як LACP і PagP вирішують одні й ті ж завдання (з невеликим відмінностями за можливостями), та краще використовувти страндартний протокол. Фактично залишається вибір між с LACP і статичним агрегуванням.

Статичне агрегування:

- Переваги:
  - Не вносить додаткову затримку при піднятті агрегованого каналу або зміні його налаштувань.
  - Варіант, який рекомендує використовувати Cisco

• Недоліки:

○ Немає узгодження настройки з віддаленої сторони. Помилки в настройках можуть призвести до утворенню петлі.

Агрегування за допомогою LACP:

• Переваги:

○ Узгодження настройок з віддаленою стороною дозволяє запобігти виникненню помилок та петель в мережі.

• Недоліки:

○ Вносить додаткову затримку при підняттю агрегованого каналу або зміні його настройок.

Висновок: Для проведення роботи, будемо використовувати роутер від виробника MicroTic, для досягнення підвищення надійності корпоративної мережі.

Література:

1. Агрегація каналів — Вікіпедія [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/Агрегація_каналів (Дата звернення: 07.04.21).
2. Основы компьютерных сетей. Тема №8. Протокол агрегирования каналов: Etherchannel / Хабр [Електронний ресурс]. - Режим доступу: https://habr.com/ru/post/334778/ (Дата звернення: 07.04.21).
3. Оліфер Н.А. «Журналы сетевых решений LAN» №02,2002 - 32 с.
4. Microsoft TCP/IP. - : Русская редакция 1999.-214с.

НОВІ ТЕНДЕНЦІЇ – 2021 ДЛЯ СУЧАСНОГО WEB-РОЗРОБНИКА

Юрковський С. С,
reliablesy@gmail.com
Черкаський державний бізнес-коледж
Оліфіренко В.М.
м. Черкаси, Україна

Кожен, хто задумувався над тим, щоб почати розвиток в кар'єрі фронтенд-програмування, стикався з такою проблемою, що гадки не має, яку мову

програмування чи фреймворк потрібно вчити. Вибрати дуже важко, тому що існує дуже багато мов та допоміжних інструментів. Для того щоб полегшити пошуки розробки з використанням JavaScript, можна виділити 3 самих популярних JS-фреймворків.

Є багато таких так званих фреймворків, але сьогодні мова піде про 3 найпопулярніших, таких як Angular, React, Vue.

Дослідження Stack Overflow 2021 року виявляє популярність фреймворків та бібліотек. Тут бібліотека React та фреймворк Vue посідають перше та друге місце відповідно. В аналогічному дослідженні 2018 року Angular перевершував React.

Результати Npm Trends показують нам зміну кількості завантажень відповідних пакетів з часом. Зокрема, на нашому графіку представлені дані за 6 місяців 2021 року. Тут ви чітко бачите, що React, з точки зору досліджуваного показника, значно перевершує своїх конкурентів. А кількість завантажень Vue, навпаки, поступово збільшується і зараз становить близько 2 млн..

NPM Trends дозволяє аналізувати не тільки кількість завантажень пакетів з NPM, але й дані відповідних проектів, взяті з GitHub. На наступному слайді показані деталі сховища для інтерфейсних інструментів, які нас цікавлять.

Використовуючи результати опитування стану JavaScript наприкінці 2020 року, ми продовжуємо порівнювати інструменти, які нас цікавлять. На наступному слайді наведено звіт, що містить інформацію про ставлення респондентів до React, Vue та Angular. Оцінюючи фреймворк або бібліотеку, вони могли вибрати різні відповіді. Наприклад, серед них є такі: "Я використовував і буду використовувати", "Я чув і хотів би вчитися", "Я ніколи не чув".

Angular, у порівнянні з іншими інструментами, можна вважати трохи більш зрілим. Навколо нього утворилася більша аудиторія користувачів. Цей фреймворк також надає розробнику багато чудових можливостей. Це, наприклад, двостороння прив'язка даних, введення залежностей, архітектура MVC, Angular CLI, підтримка TypeScript, підтримка директив тощо.

Але за останні кілька років, коли конкуренти, такі як React та Vue, зросли в популярності, Angular втратив частину своєї колишньої популярності. Причиною цього є те, що Angular є досить важким фреймворком. Це багато в чому не відповідає очікуванням програмістів. Також це особливості випуску нових версій, і обмежена підтримка SEO, і труднощі в її дослідженні. Ось чому розробники-розробники сьогодні все частіше вибирають Vue або React. Але Angular все ще використовується у багатьох популярних веб-проектах. Це, наприклад, проекти Guardian, Upwork, PayPal, Sony. Ми говоримо про великі, серйозні сайти, на яких Angular показав себе добре.

Angular варто розглянути в таких ситуаціях:

- Розробка масштабних проектів.
- Необхідність масштабованої архітектури.
- Зацікавленість у використанні TypeScript.
- Створення програми в режимі реального часу.

Відповідно до досліджень стану JavaScript, React три роки поспіль займає перше місце у всіх рейтингах. Бібліотека React була випущена Facebook у 2013 році. Метою React було виділити користувальницький інтерфейс на набір компонентів для спрощення процесу розробки. Однією з переваг React є можливість використання цієї бібліотеки для розробки власних додатків. Інші сильні сторони цієї бібліотеки включають велику спільноту, підтримку Facebook, величезну екосистему, високу продуктивність, механізми багаторазового використання компонентів та підтримку SEO-пристроїв.

React варто розглянути в таких ситуаціях:

- Створення односторінкових або крос-платформенних додатки.
- Розробка додатків малого підприємницького класу.

Vue це проект який з’явився відносно недавно, але став одним із улюблених фреймворків веб-розробників. Його популярність швидко зростає, тому що в нього не великий розмір та детальна документація.

Vue варто розглянути в таких ситуаціях:

- Створення інтелектуальних та невимогливих програм.
- Розробка програм на ранніх стадіях створення.

Висновок

Як ми можемо бачити, React та Vue обходять Angular по відсоткам «Я використовував та буду використовувати». Зараз лідирують React та Vue. Angular втрачає свою популярність, тому я б не радив починати його вивчати, а робити акцент на React або Vue, дивлячись на свої потреби.

Список використаних джерел

1) Ел.дж. https://insights.stackoverflow.com/survey/2019#most-loved-dreaded-and-wanted
2) Ел.дж - https://www.npmtrends.com/angular-vs-react-vs-vue
3) Ел.дж - https://2020.stateofjs.com/en-us/technologies/front-end-frameworks/
4) Ел.дж - https://github.com/vuejs/vue
5) Ел.дж - https://angular.io/
6) Ел.дж - https://ru.reactjs.org/

МЕРЕЖІ 6G: СТІЛЬНИКОВИЙ ЗВ'ЯЗОК НОВОГО ПОКОЛІННЯ

Шимко О. Г.,
Sasha.menshymko@gmail.com,
Черкаський державний бізнес-коледж
Холупняк К. О.
м. Черкаси, Україна

Розвиток 5G-сервісів викликав хвилю конкуренції по всьому світу і, що ще важливіше, запустив гонку з розвитку 6G.

У листопаді 2019 року була створена офіційна китайська дослідницька група щодо 6G. Розвинені країни, такі як США, Японія, Південна Корея та деякі європейські країни, почали розробляти плани досліджень і розробок для 6G, оскільки сектор телекомунікацій завжди був точкою конкуренції.

Хто б не керував сектором телекомунікаційних технологій, встановлює стандарти для продуктів та послуг і відіграє велику роль у майбутньому розвитку галузі.

Технологія 5G спрямована на створення всеосяжної сенсорної системи, в якій можна легко отримати доступ до інформації та інструментів. З іншого боку, 6G допоможе побудувати перцептивну нервову систему, що інтегрує штучний інтелект (AI) та бездротове пізнання, що може дати розумні реакції.

У порівнянні з технологією 5G, 6G матиме меншу затримку, більш високу швидкість та більшу пропускну здатність. І ця передова технологія допоможе з'єднати реальний світ з віртуальним цифровим світом. Це також зробить дизайн, науково-дослідні та дослідні розробки та експерименти значно ефективнішими та значно знизять їх витрати, дозволяючи виробляти цифрові продукти у фізичному світі за допомогою високотехнологічних технологій, включаючи 3D-друк.

Що стосується економічного розвитку, 3G сприяла електронній комерції, тоді як 4G сприяла розвитку електронної комерції та мобільних платежів. Побудова та застосування інфраструктури 5G поклало початок інтелектуальному виробництву китайських підприємств та послужило основою для швидкого розвитку сектору. Так само бездротова пізнавальна технологія, пов'язана з технологією 6G, як тільки вона дозріє, це ще більше сприятиме розвитку цифрової економіки.[1]

У цифровій економіці інтелект, заснований на великих даних, стане справжнім поштовхом до інновацій, а мережі 6G не лише стануть магістралями для передачі даних, але й набагато більш плавно інтегруватимуть крайові та основні обчислення як частину комбінованої інфраструктури зв'язку та обчислень. Це забезпечить багато потенційних переваг, оскільки технологія 6G починає працювати, включаючи доступ до можливостей AI.

Цифрова економіка на основі 6G стане визначальним фактором конкурентоспроможності країни. І технологія 6G, бездротове пізнання як її основна

характеристика, стане основною технологією та головним рушієм цифрової економіки.

Очікується, що 6G підтримуватиме швидкість до терабайта в секунду, безпрецедентний рівень ємності та затримки, що збільшить продуктивність 5G додатків, крім розширення сфери можливостей для підтримки все нових і інноваційних програм у царинах бездротового пізнання, зондування та візуалізація.

До впровадження послуг 4G Китай залишався пасивним гравцем у галузі прогресивних технологій, головним чином слідуючи за США та європейськими країнами, і не встановив стандартів телекомунікаційних технологій.

Але розвиваючи технологію 4G одночасно з розвиненою економікою, Китай став великим гравцем у цій галузі та сприяв процесу формування норм. Те, що мережа 4G в Китаї є найдосконалішою та найпоширенішою у світі, також сприяла швидкому розвитку мобільних платежів у країні.

Починаючи з 5G, китайська індустрія телекомунікацій, завдяки своєму великому науково-дослідному дослідженню, взяла на себе лідируючу позицію в галузі стандартизації та виробництва телекомунікаційного обладнання 5G.

А тепер, коли США та європейські країни відстають від Китаю в розвитку технологій 5G, вони хочуть перетягнути Китай, використовуючи неконкурентоспроможні засоби, такі як обмеження розвитку китайських компаній, таких як Huawei, та запустивши наукові дослідження та розробки в 6G перед Китаєм для отримання грошей на перевагу, якою вони користуються в промисловому ланцюзі міліметрової хвилі.

Що стосується НДДКР в технології 5G, Китай має дві переваги. По-перше, він є світовим лідером у телекомунікаційному секторі та має міцний запас талантів. По-друге, він має відносно повну промислову мережу, яка охоплює НДДКР, дизайн, виробництво та застосування, і є домом для провідного виробника обладнання 5G Huawei.[2]

Новітня історія показує, що той, хто очолює сектор телекомунікаційних технологій, встановлює стандарти для телекомунікаційних продуктів та послуг і відіграє більшу роль у майбутньому розвитку галузі.

А оскільки технологія 6G стане двигуном нового раунду економічного розвитку, уряд Китаю, підприємства та науково-дослідні організації повинні посилити співпрацю, щоб досягти успіху в конкурентній боротьбі з розвитку 6G.

Україна поступово скорочує відставання від західних країн в процесі запуску нових поколінь зв'язку. Так, якщо 3G в нашій країні з'явився в 2015 році, з відставанням від розвиненого світу в більш ніж десятиліття, то розрив між активним розвитком нашого 4G (2018 р) і європейського 4G - 5-8 років. Мережі п'ятого покоління, які в світі масово з'явилися на початку 2020 х, швидше за все, досить швидко доберуться і до нашої країни - до 2022 року.

Тому впровадження 6G, якщо воно таки з'явиться в світі до 2030-го, має торкнутися і наш ринок.[3]

Література:

1. Василь Ткаченко. Мережі та Бізнес. С. 83-87. URL: http://sib.com.ua/sib-06-115-2020/6g.html
2. Журнал HI-TECH [Електронний ресурс]. - Режим доступу: https://hi-tech.ua/catalog/
3. Інформаційний ресурс [Електронний ресурс]. - Режим доступу: https://www.pcweek.ua

СУЧАСНІ НАПРЯМКИ РОЗВИТКУ ВЕБ-ТЕХНОЛОГІЙ

Ткаченко А. Д., студент
Черкаський державний бізнес-коледж
Черниш С. В., викладач
Черкаського державного бізнес-коледжу
м. Черкаси, Україна

Кожен день у нашому житті ми користуємося такими плодами праці Web-розробників, як: соціальні мережі, інтернет-магазини, Web-додатки, прості сайти і тощо. Взагалі, під цим поняттям вважається створення сайтів, як простих, односторінкових, статичних сайтів, так і складних, насичених інтерактивністю, великим функціоналом, динамічністю [1].

Можна зазначити, що:

- Статичний сайт – це сайт, який переглядає користувач, у тій формі чи вигляді, в якому вона зберігається на сервері. Прикладом можуть бути сайт-візитка, сайт-відображення певної інформації, яка не може бути змінена користувачем і збережена на сервері.
- Динамічний, інтерактивний та функціональний сайти – це сайти, де користувач може взаємодіяти на сторінці так, як логічно дає можливість програміст, написавши код. Це сайт, в якому вміст контенту та сторінки змінюються «на льоту», у дію якого вступають всім нам відомі мови програмування, як: JAVASCRIPT, DART, ASP.NET CORE, NODE.JS, PHP, JAVA, RUBY, GO, DART тощо, а також мови запитів як SQL, GraphQL та реляційні СУБД, MySQL, Oracle [2].

Команда для розробки сайтів, зазвичай має таких спеціалістів:

1. Менеджери;
2. Web-розробники;
3. Дизайнери;
4. Тестувальники.

1) Завдання менеджерів полягає у контролюванні проекту, прийнятті рішень, які в майбутньому вестимуть стратегічний характер розвитку продукту, а також створення та впровадження комерційних автоматизацій виробничих процесів, що вигідні для компанії, мінімізуючи витрати ресурсів на придбання, налагодження і використання.

2) Web-розробники повинні задовільнити всі потреби замовника, за допомогою програмного коду, розмітки та стилів у Web-продукті, щоб для клієнта

вийшов, красивий, зрозумілий, повністю адаптивний, без багів й аномалій інтерфейс, таким, яким його зробили дизайнери, тобто із простого макета згенерувати всі картинки, всі шрифти, виявлення палітри кольорів і перенести в розмітку зі стилями. На даний момент вся робота Web-розробки ділиться на дві частини:

A. Backend;

B. Frontend.

a) Backend, як правило, відповідає за роботу тієї частини сайту, яка міститься на сервері й користувач її не бачить. У неї зазвичай обробляються дані, які користувач вводить у форму, там йде взаємодія з базою даних і загрузка файлів, зазвичай Backend-розробники використовують такі мови програмування, як: ASP.NET CORE, PHP, NODE.js, PYTHON (DJANGO), RUBY тощо, щоб ми могли здійснювати купувати в інтернет-магазині, писати коментарі та пости, робити онлайн-трансляції, дивитись відео у браузері, захистити інформацію від хакерів, та не зменшувати швидкість роботи при великому обсязі користувачів. Також можуть користуватися такими CMS як WordPress, але, як правило, швидкість та кодування їм не властиве.

b) Frontend – це те, що ми бачимо, коли заходимо на сторінку сайту, до фронтенда. Його можна розбити на такі підвиди:

- верстка сайтів по макету, тобто це люди, які чудово знають HTML, CSS і зазвичай використовують такі препроцесори, як SASS/SCSS, LESS, які пришвидшують темп роботи для розробки великих проектів, та не завжди, але використовують бібліотеки BOOTSTRAP та медіа запроси.

- Та простих розробників, які пишуть логіку сайтів і контролюють, щоб результат коректно відображався на різних пристроях; щоб кнопки використовували свої функції, наприклад, коректно вводить дані та перероблювати їх, включати відео/музику та включати автоматично інший контент, шукати результат у пошуковому рядку тощо. Вони пишуть багато логіки сайту на JS, GO, DART і тому

подібних, користуються системами контролю версій (наприклад, GIT та репозиторій GitHub) та збірниками проектів, модулів (WebPack, GULP…). На сьогодні, сайтом можна вважати Web-додаток.

Також є і Fullstack спеціальності. Це люди, які працюють одночасно з двома сторонами. Їх вважать різносторонніми людьми, які знають верстати, програмують, працюють із серверами. Вони завжди вчать нові технології, які з'являються, нові стандарти…

3) Дизайнери, як правило, чудово володіють фотошопом, можуть створювати макети на них чи на конструкторів сайтів, таких як: Figma, Axure. Знають, як зробити логотип, наприклад, на Adobe Illustrator, їхня задача створити макет та передати програмісту для перенесення створеного у робочий код.

4) Тестувальники зазвичай тестують результат, чи результати програмістів, шукають Баги, повідомляють про можливі фічі, щось придумують, перевіряють [1].

Сучасні заробітні плати Web-розробників в Україні (За даними сайту Work.ua):

- Мінімальна заробітна плата — 9000 ₴;
- Середня заробітна плата — 22500 ₴;
- Найвища заробітна плата — 51000 ₴.

Сучасні тренди, які край необхідні для Web-розробки у 2021 році (деталі на сайті: motocms.com):

1) Progressive Web Apps (PWA - прогресивні веб-додатки);
2) Чат боти та штучний інтелект;
3) Блокчейн;
4) Motion UI – анімація та переходи;
5) Еренди веб розробки: SSL протокол і HTTPS;
6) Google AMP сторінки;
7) Відстеження поведінки користувачів;
8) Тренди веб розробки VR і AR;

9) WordPress 5.3.2 Нова версія [3].

ЛІТЕРАТУРА

1. Сучасні напрямки розвитку веб-технологій [Електронний ресурс] // Професія Веб розробник: хто це? GeekBrains. 2020. Режим доступу до ресурсу: https://www.youtube.com/watch?v=QuH3P3KLmqQ.
2. Сучасні напрямки розвитку веб-технологій [Електронний ресурс] // Статичні та динамічні web-сайти. 2018. Режим доступу до ресурсу: https://webstudio2u.net/ua/site-develop/444-interactive-site.html.
3. Сучасні напрямки розвитку веб-технологій [Електронний ресурс] // Новини, тенденції і тренди веб розробки в 2020 рік. 2020. Режим доступу до ресурсу: https://www.motocms.com/blog/ru/trendy-web-razrabotki/.

Секція 5.

Кібернетична безпека

ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА. КІБЕРБЕЗПЕКА, ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Ільченко Є.І.
Черкаський державний бізнес-коледж
Черниш С.В.

Становлення інформаційного суспільства не лише дає змогу будувати більш ефективне та успішне суспільство, але й надає нових імпульсів традиційним загрозам безпеки держави та створює принципово нові складнощі для системи національної безпеки. В таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору. З огляду на рівень проникнення ІКТ у всі критично важливі сфери життєдіяльності людини та держави, таку можливість надає протистояння у кіберпросторі та ведення кібервійн.

Україна потребує створення адекватної системи безпеки у світі, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз.[1].

В Україні в системі забезпечення кібербезпеки держави задіяно низку військових та правоохоронних органів. Серед яких Міністерство оборони України (та його спеціальні підрозділи – зокрема Головне управління розвідки), Служба безпеки України та т.і. Водночас, діяльність цих відомств не завжди відповідним чином забезпечується.

За ефективністю та наслідками застосування кіберзброї, а саме такий термін все частіше використовують вчені, можна прирівняти до зброї масового ураження. Тому кібербезпека — одна з основних проблем, що викликає занепокоєння.

Чотири роки тому Росія розв’язала проти України гібридну війну. Цей тип війни передбачає, що країна-агресор може залишатися публічно непричетною до такого конфлікту та проводити приховані військові операції. Ряд провідних експертів Заходу небезпідставно називають її ще як «війна нового покоління» або «війна нової генерації». [6]

Отже, функціонування та захист вітчизняного як інформаційного, так і кіберпростору є важливим завданням держави в умовах проведення військових дій з Росією на Сході нашої країни [4]

Відомо, що за останні роки різні сектори української економіки та й суспільне життя пересічних громадян стали дуже вразливими у кіберпросторі. Постійно страждають від періодичних кібератак державні та приватні компанії, до яких вони зовсім, як виявилося, не були готові. Шкода, але доводиться констатувати також той факт, що Україна немає навіть й сьогодні будь-яких дієвих інструментів для запобігання атак і їх ефективній протидії, а всі наявні заходи кіберзахисту, в основному, є безсистемними і, як наслідок, безуспішними.[3]

Загроза кібербезпеці держави у вигляді кіберінтервенції може бути як зовнішньою, так і внутрішньою.

Крім того, кожне суспільство потребує правил, стандартів, норм, положень, інструкцій та інших документів, щоб почувати себе захищеним у кіберпросторі хоча б у правовому відношенні. Зараз з'являються галузеві нормативні документи, що стосуються кіберризиків, зростає інтерес до цієї галузі з боку законодавчих органів. В Україні розробляються стандарти з безпеки для об'єктів критичної інфраструктури.

Головною метою "Стратегії кібербезпеки України" (один з основополагаючих законодавчих документів) є створення умов для безпечного функціонування кіберпростору держави, його використання в інтересах суспільства і особи. Документ також передбачає комплекс заходів, спрямованих на боротьбу із кіберзагрозами, поглиблення міжнародного співробітництва у цій сфері, забезпечення захисту державних електронних інформаційних ресурсів та інформаційної інфраструктури. Задля реалізації цієї стратегії РНБО утворило Національний координаційний центр кібербезпеки як робочий орган Ради.[5]

Література:

1. В мире два десятка стран занимаются кибероружием – McAfee // Cybersecurity.ru.
2. MilitaryandSecurityDeploymentsInvolvingthePeople'sRepublicofChina.
3. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011
4. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.
5. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" / Указ Президента України від 1 трав. 2014 р., № 449/2014. [Електронний ре- сурс]. – Доступний з http://www.prezident.gov.ua
6. Войціховський, А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн [Електронний ресурс] / А. В. Войціховський // Журнал східноєвропейського права. - 2018. - № 53. - С. 26-37.

FEATURES OF CONSTRUCTION OF STEGANOGRAPHIC SYSTEMS

Demchenko I.
Cherkasy State Business College
Zakharova M.V.

The task of protecting information from unauthorized access in one way or another has been solved throughout human history. In the process of studying steganography, it becomes clear that it is, in fact, not something new. In the last decade, thanks to the widespread use of multimedia technologies and telecommunications, the development of steganography has reached a fundamentally new stage, which experts call

computer steganography (CS). Among the main areas of use of CS: hiding (by embedding) messages in digital data, which are usually analog in nature (language, images, audio or video). For example, the least significant bits of a digital image or audio file can be replaced with data from a text file so that an independent third-party observer will not detect any loss in image or sound quality. Therefore, the purpose of this work is to determine the features of the construction of steganographic systems.

Steganographic system or, in short, steganosystem - is a set of tools and methods used to form a hidden (invisible) channel of information transmission. In other words, it is a system that performs the task of embedding and separating messages from other information [1]. Moreover, the process of hiding data, like the process of compression (compression), is different from the encryption operation. Its purpose is not to restrict or regulate access to the signal (file) -container, but to largely ensure that the embedded data remains intact (unmodified) and recoverable.

The following provisions must be taken into account when constructing the thigh system: - the steganosystem must have an acceptable computational complexity of implementation (computational complexity means the number of steps or arithmetic-logical operations required to solve a computational problem, in this case - the process of embedding / retrieving hidden information to / from the container signal);

- the necessary bandwidth must be provided (which is especially relevant for steganosystems of latent data transmission); - methods of concealment must ensure the authenticity and integrity of classified information for the authorized person; - the potential violator has a complete idea of the thigh system and the details of its implementation. The only thing he does not know is the key with which only its owner can establish the existence and content of the hidden message; - if the fact of existence of the hidden message becomes known to the infringer, it should not allow the last to extract it as long as the key is kept secret; - the infringer must be deprived of any technical and other advantages in the recognition or, at least, the disclosure of the content of classified messages [2].

Today, thigh systems are actively used to solve the following key tasks: - protection of confidential information from unauthorized access; - copyright protection of intellectual property; - overcoming the systems of monitoring and management of network resources; - "camouflage" software; - creation of information leakage channels hidden from the legitimate user [1].

Thus, the paper examines the features of the construction of steganographic systems, identifies areas of application of steganography, namely copy protection (e-commerce; control of duplication; dissemination of multimedia information (video on request)), hidden annotation of documents (medical images; cartography; multimedia databases). data), authentication (video surveillance systems, e-commerce, voice mail; electronic confidential record keeping), for covert communication (use for military and intelligence purposes, as well as in cases where cryptography cannot be used).

References:

1. Computer steganographic processing and analysis of multimedia data: a textbook. / G.F. Konakhovich, D.O. Progonov, O.Yu. Puzirenko. - Kyiv: "Center for Educational Literature", 2018. - 558 p.

2. Khoroshko V.O., Azarov O.D., Shelest M.E., Yaremchuk Y.E. Fundamentals of computer steganography: Textbook. way. for students and graduate students. - Vinnytsia: VSTU, 2003.

3. Gustavus J. Simmons, The Prisoner's Problem And The Subliminal Channel, Advances in Cryptology: Proc. Workshop on Communications Security (Crypto'83, David Chaum, ed.), Plenum Press, 1984, pp. 51-67.

MONITORING OF CYBER SECURITY SYSTEMS

Teplyi E.
Cherkasy State Business College
Zakharova M.V.

The introduction of an information security event monitoring system will allow the company to achieve the following advantages:

• provide centralized management of IS events and incidents;

• increase the speed of detection, investigation and response to incidents;

• manage IS incidents; • increase the effectiveness of IS risk management;

• increase compliance with policies and regulations.

Also for effective protection of information, one of the main components is the presence of an operational security center. The Security Operations Center is a centralized unit of the institution that deals with information and cybersecurity issues at the organizational and technical level. An operational security center is a facility where corporate information systems (websites, applications, databases, data centers, servers, active network equipment, computers, and other terminal equipment) are monitored, evaluated, and protected. The primary function of the OCB is analysis based on the current monitoring of information security events. Priority is given to detecting alarms, responding to security incidents and correcting the consequences of each monitored event [1]. The choice of methods and objects of monitoring the system and network depends on many factors - the configuration of the system, services operating in it and services, the configuration of servers installed on them P3, the capabilities of P3 used for monitoring.

At the most general level we can talk about such elements as:

• checking the physical availability of equipment;

• checking the status (efficiency) of services and services;

• detailed check of not critical, but important parameters of system functioning - productivity, loading, etc.

The initial verification steps may be to test the physical availability of the equipment, which may be disrupted by the disconnection of the equipment itself or the failure of telecommunications channels.

The next step is to test the performance of critical services. In most cases, it is desirable to check not only the fact of response of the service or service, but also the delay of the response. However, this applies to the next most important task - load verification. In addition to the response time of devices and services for different types of servers, there

are other fundamentally important checks – memory and CPU usage of the web server, database server, disk space of the file server. The essence of network security monitoring is to identify abnormal events in its operation. Signs of a network attack are abnormally high levels of CPU usage, a sudden reduction in disk space, a sharp increase in network traffic. Accumulation of error messages in server log files or server OS event log helps to detect repeated or systematic failures. Unwanted changes to access rights to a resource or file content may indicate an intruder. When configuring the monitoring system, two opposing requirements should be taken into account: a sufficient number of inspections should be performed to ensure a high degree of monitoring reliability, while not being overwhelmed by this number to avoid overloading the equipment and specialists responsible for analyzing the results [2].

Thus, the development of an information security monitoring system, the selection of the required number and types of security checks is a serious engineering task that requires a careful approach. When configuring the information security monitoring system, it is necessary to perform a sufficient number of checks. this will ensure a high degree of reliability and avoid congestion.

References:

1. Sitnik VF Decision support systems: textbook. manual - Kyiv: KNEU, 2009. - 614p.
2. Kovtunets VV, Nesterenko OV, Savenkov OI Security of decision support systems: textbook. manual Kyiv: National Academy of Management, 2016. —190p.

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Кущій С. С.
sonya.kushchiy@gmail.com
Харківський національний економічний університет ім. Семена Кузнеця
Наумік-Гладка Катерина Георгіївна
доктор економічних наук, професор

Харківський національний економічний університет ім. Семена Кузнеця

В нинішній час, люди стикаються з порушенням безпеки кожен день. Хотілося б відзначити, що за результатами дослідження Norton Cybercrime Report, одного з найбільших в світі досліджень в сфері кіберзлочинів, 83% користувачів мережі інтернет стурбовані конфіденційністю своїх даних. Така стурбованість є цілком виправданою - за даними за 2019 рік, в 16 країнах зафіксовано 800 мільйонів жертв кіберзлочинності [2].

Проблема кіберзлочинності є як ніколи актуальною, оскільки найчастіше це здійснюється з метою: нанесення економічних збитків у вигляді крадіжки грошових коштів та конфіденційної інформації, до нанесення шкоди державним і політичним інститутам. Також - поширення ідей та ідеологій з метою вербування інтернет-користувачів в ряди, наприклад, терористичних і націоналістичних угруповань, нанесення морального, психологічного шкоди громадянам.

Подібні проблеми кіберзлочинності завдають істотної шкоди і безпосередньо несуть загрозу міжнародній безпеці, головною метою якої є дотримання всіма державами загальновизнаних принципів і норм міжнародного права, виключає вирішення спірних питань і розбіжностей між ними за допомогою сили або загрози.

Сьогодні, цифрові технології «колонізували» наше повсякденне життя. Людство купує товари в онлайн-магазинах, користуються мобільним банкінгом, використовують соціальні мережі для ведення бізнесу, замовляють квитки або готель онлайн. Тому можна стверджувати, що більшість вже живуть «в цифрі».

Безумовно, цифрове середовище спрощує життя і звичну діяльність, вивільняючи час для важливих цінностей - сім'ї, подорожей, хобі та відпочинку. Адаптуватися і ефективно користуватися досягненнями цифровізації можуть вже багато, особливо зараз, в період карантину всі приєднуються до онлайн-формату отримання освіти, роботи, здійснення покупок і так далі. Але, з точки зору безпеки, даний вид електронної комунікації виключно вразливий - за допомогою технічних

засобів з комп'ютерів можна заволодіти будь-якою інформацією. Існують, звичайно, способи захисту, але 100% гарантії, що вони спрацюють, немає. За таких умов виникає необхідність забезпечення безпеки основних інструментів цифрової економіки - захист електронних підписи, платежів, токенов, sim-карт, online-сервісів, захист інформації в електронних хмарах, базах даних, розвиток криптографії та технологій аутентифікації особи, захист системи електронного документообігу, захист серверів і так далі [3].

Некомерційний форум з інформаційної безпеки, який описує себе як «провідний світовий авторитет в області кібербезпеки, інформаційної безпеки та управління ризиками», попереджає в своєму щорічному дослідженні Threat Horizon про підвищений потенціал проблем, а саме: збоїв в роботі, погіршення контролю власної інформації [1].

Основними загрозами кібернетичної безпеки на порядку денному є: фішинг, а саме фішингові атаки, які ретельно передаються цифровими повідомленнями для установки шкідливого ПО або розкриття конфіденційних даних. Коли співробітники в більшості організацій більше обізнані про небезпеки фішингу, хакери підвищують ставку - наприклад, використовуючи машинне навчання, щоб набагато швидше створювати і поширювати переконливі підроблені повідомлення в надії, що одержувачі мимоволі поставлять під загрозу мережі і системи своєї організації.

Також стратегії программ-вимагачів мають тенденцію розвиватися. Вважається, що атаки програм-вимагачів щорічно обходяться жертвам в мільярди доларів, оскільки хакери використовують технології, які дозволяють їм буквально викрадати бази даних окремих осіб або організацій і зберігати всю інформацію для отримання викупу.

Кріптоджекінг, що являє собою рух криптовалюти, також впливає на кібербезпеку. Наприклад, кріптоджекінг - це тенденція, при якій кіберзлочинці захоплюють домашні або робочі комп'ютери третіх осіб, щоб «добувати» криптовалюту [4]. Оскільки майнінг криптовалюти (наприклад, біткоїнів) вимагає

величезних обчислювальних потужностей комп'ютера, хакери можуть заробляти гроші, таємно копіюючи чужі системи.

Кіберфізичні атаки, технологія, яка дозволяє модернізувати і комп'ютеризувати критично важливу інфраструктуру, також несе ризик. Постійна загроза зломів електричних мереж, транспортних систем, водоочисних споруд і т. д. Згідно з недавнім звітом The New York Times, навіть багатомільярдні військові системи Америки знаходяться під загрозою високотехнологічної нечесної гри [1].

Актуальною проблемою є і атаки, спонсоровані державою. Крім хакерів, які прагнуть отримати прибуток за рахунок крадіжки індивідуальних і корпоративних даних, цілі держави тепер використовують свої кібер-навички для проникнення в інші уряди і проведення атак на критично важливу інфраструктуру. Згідно зі звітом Thomson Reuters Labs: «Кібератаки, спонсоровані державою, є новий і значний ризик для приватних підприємств, який все більше кидає виклик тим секторам ділового світу, які надають зручні цілі для вирішення геополітичних проблем» [1].

Не можна не згадати і інтелектуальні медичні пристрої та електронні медичні записи. Галузь охорони здоров'я все ще знаходиться в процесі серйозної еволюції, так як більшість медичних карт пацієнтів тепер переведені в онлайн, а медичні працівники усвідомлюють переваги досягнень в області інтелектуальних медичних пристроїв. За даними Інституту програмної інженерії Університету Карнегі-Меллона: «У міру того, як все більше пристроїв підключається до мереж лікарень і клінік, дані та інформація пацієнтів будуть ставати все більш уразливими» [1]. Оскільки лікарні та медичні установи все ще адаптуються до оцифрування медичних карт пацієнтів, хакери використовують безліч вразливостей в своїх засобах захисту. А тепер, коли медичні карти пацієнтів майже повністю доступні в Інтернеті, вони є основною метою для хакерів через міститься в них конфіденційної інформації.

В останні роки епідемія кіберзлочинності швидко загострилася, в той час як компанії та уряди щосили намагалися найняти достатньо кваліфікованих фахівців

для захисту від зростаючої загрози. Очікується, що ця тенденція збережеться в 2021 році. Гостра нестача кваліфікованих фахівців у галузі кібербезпеки продовжує бути причиною для занепокоєння, тому що сильний, розумний цифровий робочої сили має важливе значення для боротьби з більш частими, більш складні кібербезпека загрози, які виходять зі всієї земної кулі.

Література:

1. Moore M. Cybersecurity Threats in 2020 [Електронний ресурс] / Michelle Moore // University of San Diego – Режим доступу до ресурсу: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/
2. 2019 Norton Cyber safety insights report global results [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2019-nortonlifelock%20-cyber-safety-insights-report-global-results-en.pdf
3. Бородакий Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов. // Концептуальные аспекты кабербезопасности. – 2013. – С. 2–9.
4. Гарнаева М.А., Функ К. Kaspersky security bulletin 2013 // Вопросы кибербезопасности. 2014. №3. С. 65-68.

PECULIARITIES OF DIGITALIZATION: A FACTOR OF ENSURING ECONOMIC SECURITY OR BASIS FOR THE DEVELOPMENT OF CYBERCRIME

Harkusha V. O.
garkusha_vladyslava@ukr.net
International Economic Relations Department
Simon Kuznets Kharkiv National University of Economics
Naumik-Gladka K. G.,
Doctor of economic sciences, professor
Simon Kuznets Kharkiv National University of Economics

Introduction. At the present stage of transition to a qualitatively new type of social system - the information society -, there is a profound transformation of the functioning of the global economy. These changes are especially noticeable against the background of the exponential strengthening of globalization, digitalization, social transformation, economic integration, and social change, which emphasizes the importance of studying the features of digital digitalization as a factor in ensuring economic security or the basis for cybercrime.

Analysis of recent research and publications. The materials of the research allow us to state that several fundamental types of research of foreign and domestic scientists have been devoted to the study of threats, challenges, approaches to the interpretation of the concept and ways of solving cybersecurity problems, as well as prospects of digitalization of modern society. Among the scientific works should be distinguished the works of such scientists: M. Bezkorovainy, A. Tatuzov, V. Makarov, A. Bakhtizin, M. Burilina, A. Zgoba, D. Markelov, P. Smirnov. However, the rapid changes that cover all spheres of society, necessitate a systematic, comprehensive study of modern aspects of digitalization, cybersecurity and the development of digital technologies, which are not fully disclosed and in the available works are covered in fragments.

The purpose of the work is to develop a theoretical and methodological justification of the characteristics of digital technologies and determine their role in ensuring economic security or the formation of cyber threats in the information space.

Main part. First of all, it is important to note that in today's conditions of cyberwars between states, cybercrime in the commercial sector, attacks on government databases, digitalization, and digital technologies are indeed becoming a significant threat to cybersecurity, a tool of cybercrime and the basis for financial pyramids. and machinations [3, p. 87]. For optimal analysis of the features of digitization processes, I think it is advisable to use an advanced method of SWOT-analysis (Table 1), where Z is the estimate; P - importance; V - significance (Z × P) [1, p. 55].

Table 1

SWOT-analysis of features of digitization processes in modern conditions

Strengths U = 294	**Weaknesses U = 125**
S1: Availability of a single information space for continuous data exchange between various fields of activity and structural divisions (Z=7, P=8, V=56). **S2:** Virtualization of the main production facility (Z=8, P=10, V=80). **S3:** Continuous management of data about objects throughout their entire life cycle, including the automatic collection, accumulation, modification and analysis of information, as well as the generation of such data (Z=5, P=8, V=40). **S4:** Digitalization makes possible advanced management through Big Data (Z=6, P=6, V=36). **S5:** Overcoming polypolarity (Z=5, P=6, V=30). **S6:** ML algorithms (Z=4, P=4, V=16). **S7:** Development of economic interdependence and security (Z=4, P=5, V=20). **S8:** Operational interaction of geographically distributed employees via the Internet (Z=4, P=4, V=16).	**W1:** Excessive politicization, populism (Z=6, P=8, V=48). **W2:** Erosion of European security, growing stockpiles of weapons of mass destruction (Z=5, P=7, V=35). **W3:** Increasing economic gap and social disunity between countries, peoples and social groups (Z=4, P=5, V=20). **W4:** The conquest of new markets by TNCs is accompanied by the destruction of entire industries in all regions of the world. The consequences are unemployment, underemployment of almost 1 billion people. Most of them live in the poorest countries. (Z=4, P=4, V=16). **W5:** Deficit of resources in the conditions of overpopulation of the planet (Z=2, P=3, V= 6).
Opportunities U = 129	**Threats U = 161**

O1: Guarantee of the efficiency of production, innovations, scientific and technical progress due to digitalization (Z=5, P=9, V=45). **O2:** Globalization and democratization (Z=6, P=7, V=42). **O3:** Accumulation of social wealth by creating an efficient economy; with the creation in society of the unity of interests, consent and personal responsibility of each citizen for the common good and international security (Z=4, P=8, V=32). **O4:** Discoveries in the field of genetics, medicine, AI, smart household items create an unprecedented number of opportunities to improve, facilitate, prolong the lives of the population (Z=2, P=5, V=10).	**T1:** Geopolitical, military, nuclear threats, terrorism (contradictions in Europe, Turkey, the Middle East, EU relations with NATO (Z=5, P=6, V=30). **T2:** Techno-economic blocs, global competition (Silicon Valley in the US, China, post-Soviet countries - the market for outsourcing) (Z=4, P=6, V=24). **T3:** Environmental threats (Z=5, P=7, V=35). **T4:** Demographic threats (Z=5, P=6, V=30). **T5:** Economic and financial threats to the population, entrepreneurial activity: shadow economy, financial fraud, cross-border capital inflows (Z=6, P=7, V=42).

Source: developed by the author using [2, p. 137].

The calculated results of peculiarities of digitization processes in modern conditions are shown in Fig. 1.

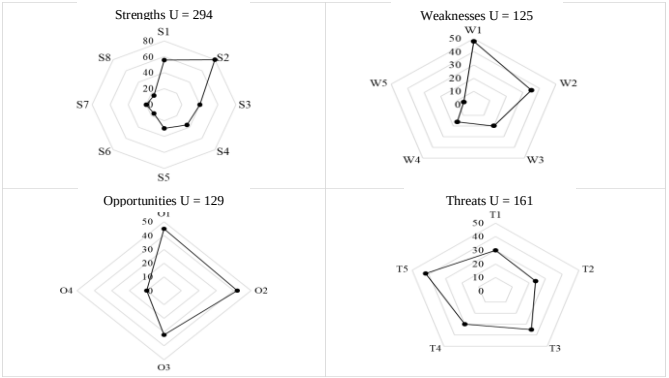


Fig. 1. Results of peculiarities of digitization processes in modern conditions

Source: developed by the author.

Conclusion. Thus, it is essential to conclude that the peculiarities of digitalization do indicate the spread of cybercrime in the information space, Internet fraud, and financial fraud, but the obvious positive effect of the introduction of digital technologies is much greater, promotes innovation, e-business, globalization, expanding markets and business opportunities. The onset of the era of digitalization raises high expectations for many. Some people fear that artificial intelligence as the core of digitalization will lead to job losses, higher unemployment, and social instability. However, statistics in recent years show that in no country has digitalization significantly affected economic growth and the dynamics of national labor productivity. Modern economies rely heavily on critical infrastructure, including transport, communications, energy supplies, and the Internet (the fight against cyber-crime). However, actions against private and public IT systems have shown that cybercrime is a potential new economic, political and military weapon. Information networks become the main resource of power in society, and the main tool of political influence is the technology of manipulating symbols and "cultural codes". Media texts have great potential to influence the minds and feelings of a mass audience. On the one hand, they can educate people, promote freedom and social justice, but on the other hand, they can enslave people, misinform them, incite ethnic conflicts, and sow distrust and fear. Potential problems in the interaction of people with AI do not mean that cyber technologies and robotics should not be developed, on the contrary, this means that it is necessary to foresee upcoming threats and manage the process.

Literature:

1. Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T. & Aljaaf, A. J. (2020) “Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyberattacks”. Studies in Computational Intelligence, vol. 855: 47-76.

2. Azvine, B. & Jones, A. (2019) “Meeting the future challenges in cybersecurity”, Industry 4.0 and Engineering for a Sustainable Future, pp. 137-152.

3. Benjamin, V., Li, W., Holt, T., & Chen, H. (2015) “Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops”, 2015 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 85-90.

КІБЕРБЕЗПЕКА В ОСВІТІ

Нога М.С
Черкаський державний бізнес-коледж
Холупняк К.О, викладач І категорії

Навчальним закладам необхідно зробити кібербезпеку пріоритетом. Незважаючи на те, що цей сектор стикається з великими проблемами, такими як брак персоналу та брак фінансування та ресурсів, кібератаки є не менш частою або менш серйозною освітою. Насправді вони, здається, щорічно набирають позиції у поширеності, оскільки про випадки порушень у школах та вищій освіті широко повідомляються.

Більш тривожними є порушення, коли безпека студентів порушена. Навчальним закладам доручено захищати своїх учнів, багато з яких є неповнолітніми, але слабка інфраструктура кібербезпеки може поставити їх під загрозу.

Це стало дуже зрозумілим, коли відеоспостереження в кількох школах Блекпула нібито було порушено, а кадри, як повідомляється, транслюються в Інтернеті.

Прикро, що хоча кібербезпека в освіті необхідна для захисту від фінансових втрат і запобігання зривів, також важливо захистити учнів від шкоди.

Ось чому сектору потрібно зробити все можливе, щоб забезпечити захист їх програм і систем, а також працювати над подоланням будь-яких проблем.

Оскільки місця проведення освіти різняться за розмірами, призначенням та зростом, мотиви нападу можуть також відрізнятися. Наприклад, те, що може бути загальною загрозою для всесвітньо відомих університетів / коледжів, не може бути

проблемою для шкіл чи шкільних округів. Отже, установам необхідно оцінити ризик та зрозуміти, які дані є вразливими для несанкціонованого доступу.[1]

DDoS-атаки – розповсюджені відмови в обслуговуванні або DDoS-атаки є поширеним типом атаки на всіх рівнях навчального майданчика. Ось де мотив зловмисника полягає в тому, щоб спричинити широке порушення роботи мережі інституту, що негативно впливає на продуктивність праці.

Це може бути відносно легким нападом для кіберзлочинців-любителів, особливо якщо цільова мережа погано захищена.Були випадки, коли студенти чи викладачі успішно здійснювали DDOS-атаку, мотиви - від простого бажання вихідного дня - до протестування способу розгляду скарги.

Крадіжка даних - це ще одна атака, яка зачіпає всі рівні освіти, оскільки всі заклади зберігають дані студентів та працівників, включаючи важливі деталі, такі як імена та адреси. Цей вид інформації може бути цінним для кіберзлочинців з кількох причин, незалежно від того, чи планують вони продати інформацію третій особі або використовувати її як інструмент торгів та вимагати гроші.

Важливим аспектом цього типу атак є те, що хакери можуть залишатися непоміченими протягом тривалих періодів часу. Як це було в Берклі, де протягом кількох місяців з комп'ютерів університету було викрадено щонайменше 160 000 медичних записів.

Фінансовий прибуток - ще одним мотивом хакерів, які здійснюють напад на навчальний заклад, є фінансові вигоди. Це може бути не надто великим ризиком для державних шкіл, але приватні установи та університети / коледжі, що займаються великою кількістю студентських зборів, є головною ціллю для кіберзлочинців.

Сьогодні зазвичай школярі або батьки платять збори через інтернет-портал, часто перераховуючи великі суми грошей на весь термін навчання або рік навчання. Без належного захисту чи підготовки з боку освітніх установ це є слабким місцем для перехоплення кіберзлочинців.

Шпигунство - четверта причина, чому освіта є ціллю кіберзлочинності, - це шпигунство. У випадку з вищими навчальними закладами, такими як Університети / Коледжі, вони часто є центрами досліджень та володіють цінною інтелектуальною власністю.

Університети / коледжі повинні бути належним чином захищені, оскільки вважається, що наукові, інженерні та медичні дослідження університетів Великобританії раніше були піддані компромету хакерам, і багато часу та коштів для фінансування їх професіонали часто стоять на чолі цих атак.

Фішинг - фішинг-шахрайства часто набувають форми електронного листа або миттєвого повідомлення і розроблені для того, щоб змусити користувача довіряти джерелу в шахрайській спробі отримати доступ до своїх облікових даних - будь то чутливі дані студентів чи конфіденційне дослідження.

Цей тип нападу виділяється як головна загроза, яка стикається з місцями вищої освіти, що пропонує хакерам регулярно націлювати сектори за допомогою методу.

Зловмисне програмне забезпечення, як правило, заражає пристрої, що використовують троян, файл або додаток, замасковані, щоб виглядати законними. Однак було показано, що деякі викупні програми (наприклад, атака WannaCry) пересуваються між пристроями без взаємодії з користувачем.[2]

Відсутність обізнаності - загроза, яку перелічують професіонали як у подальшій, так і у вищій освіті, - це недостатня обізнаність чи нещасні випадки. Це може бути з боку персоналу чи студентів, які недостатньо навчені практикувати добру кібергігієну або випадково поставити під загрозу мережу.

Незважаючи на різні прояви, людські помилки відіграють ключову роль у кожній з цих трьох загроз кібербезпеки в секторі освіти. Однак, завдяки кращому загальному навчанню з питань кібербезпеки та усвідомленню мотивів та методів нападників, навчальні майданчики могли б краще захистити себе від кібератак.

Однак сектор також стикається з проблемами, які перешкоджають прогресу.

Проблеми, з якими стикається освіта

Звіт JISC також досліджує проблеми, які стоять перед IT-спеціалістами щодо захисту освітніх мереж. На запитання оцінити, наскільки добре захищений їхній навчальний заклад за шкалою від 1 (зовсім не до 10) (дуже добре), подальша освіта набрала нижче загальної, ніж вища. Середній бал для закладів подальшої освіти становив 5,9, а для вищої - 7,1.

Обґрунтування нижчих балів включало:

- брак ресурсів та бюджету - потенційно вказує на брак фінансів для вкладень у кібербезпеку, будь то програмне забезпечення чи персонал.
- відсутність політики - визначення політик щодо використання мережі та забезпечення їх дотримання може бути складним у великих установах з динамічною сукупністю користувачів.

Незважаючи на ці виклики, все ще слід очікувати, що сектор освіти захистить свої мережі від несанкціонованого доступу та кіберзагроз. Особливо, коли наслідки можуть бути такими ж серйозними, як приклади, про які ми говорили раніше.

Але є кілька критичних кроків, які повинна здійснити кожна установа, щоб закласти основи безпечної IT-мережі.

У зв'язку з недостатнім фінансуванням та нестачею ресурсів, сектор освіти повинен зосередити свої зусилля на мінімізації ризику кібератаки, а не на реактивне ставлення після такого.

Забезпечення базової підготовки для всіх користувачів вашої мережі - це один із способів пом'якшити наслідки нестачі фінансування та ресурсів.

Це може бути настільки просто, як обмін посібником з працівниками та студентами, включаючи інформацію про те, на що слід звернути увагу, та поради щодо практичної належної гігієни кібербезпеки. Надання людям необхідної інформації для захисту мережі в усіх точках доступу може зменшити кількість випадків, спричинених помилками людини.

Ще одним економічно ефективним способом захисту безпеки вашого закладу та його учнів є реалізація зручного для користувача інструменту багатофакторної аутентифікації (MFA).

Це лише деякі з рентабельних способів захисту школи, університету чи коледжу від будь-якої форми несанкціонованого доступу. Зі збільшенням частоти та потенційної серйозності кібератаки ставляться до сектору освіти, важливо, щоб IT-фахівці могли працювати над тим, щоб знайти рішення таких проблем, як брак фінансування.[3]

Література:

4. Інформаційний ресурс [Електронний ресурс]. URL: https://biz.ligazakon.net/news/198704_v-ukran-rozpochavsya-msyats-kberbezpeki-2020
5. Швидкий пошук надійних рішень і практичної інформації uteka [Електронний ресурс]. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-samye-populyarnye-sposoby-moshennichestva-v-elektronnoj-kommercii
6. Інформаційний ресурс [Електронний ресурс]. URL: https://infotel.ua/ua/IT-bezopasnost-i-zacshita-informatsii-1/

ВИДИ, НАСЛІДКИ ТА СПОСОБИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Циганенко Д. О.
denistsyganenko00@gmail.com
Київський національний університет технологій та дизайну
Оліфіренко В. М.
м. Черкаси, Україна

В сучасному світі практично неможливо знайти сферу, в якій не використовуються сучасні інформаційні технології. Комп’ютери та комп’ютерне устаткування займають ключове місце в усіх сферах суспільства, виконуючи різні функції у роботі та повсякденному житті. Інформаційні технології це один із сучасних способів спілкування, головними перевагами якого є загальнодоступність.

Одним із інструментів Інформаційні технології, який набуває широкої популярності в світі виступає віртуальний простір. Віртуальний простір запозичає все із реального світу, не тільки хороше, а й не дуже. Подекуди інтернет простір стає місцем злочину та його інструментом.

Інтернет злочини відноситься до окремого виду інтернет загроз – кіберзлочин. Кіберзлочинність має безліч різновидів. Банківські рахунки, паролі, дані платіжних карток, персональні дані, особиста інформація фізичних та юридичних осіб є об'єктами кіберзлочинів . Нині кіберзлочинність є одним з найпоширеніших видів злочинів і їх кількість стрімко збільшується. Найголовнішою причиною стрімкого темпу їх зростання є велика прибутковість. Внаслідок окремих кіберзлочинів, злочинці отримують великі суми неправомірної грошової винагороди. Ще одним із чинників реальної загрози є анонімність, яка дозволяє протиправні дії з будь-якого куточку світу. Що в свою чергу ускладнює пошук та виявлення зловмисників.

Жертвою кіберзлочинів може стати будь-хто, хто має доступ до мережі інтернет. Сьогодні існує безліч схем та інструментів, якими користуються інтернет-злочинці, найпоширенішими з них є:

1) Кардинг – махінації з даними платіжних карток та систем.
2) Фішинг – підміна сайту чи веб-сторінки.
3) Вішинг – заволодіння конфеденційними даними власника картки, за допомогою телефонних дзвінків під виглядом працівника банку.
4) Онлайн-шахрайство – створення фіктивних інтернет-магазинів, імітація продажу товарів чи послуг.
5) Піратство – незаконне використання чи розповсюдження інтелектуальної власності.
6) Кард-шарінг –зламування доступу для перегляду супутникового та кабельного телебачення.

7) Соціальна інженерія – інструмент для маніпулювання та управління людиною.
8) Мальваре – створення та розповсюдження шкідливого ПО.
9) Розповсюдження протиправного контенту – інформації, яка пропагує екстремізм, тероризм, наркоманію, і насильство.[1]

Основним фактором, який відіграє найбільшу роль в успішності кібератак є саме людський фактор. Дотримуючись персональних правил захисту ви зможете перетворити слабкість людського фактору на перевагу, що слугуватиме надійним захистом. Існує декілька порад щодо захисту себе від кіберзлочинів:

1) Встановлення на комп'ютер антивірусного ПО та його оновлення.
2) Створення паролів з різними цифрами, знаками та спеціальними символами, а також періодична їх зміна.
3) Не використовувати однаковий пароль на всіх сайтах, пристроях.
4) Зберігання резервних копій даних на пристроях, що не мають доступу до мережі.
5) Запобігання викраденню особистої інформації.

Ці правила та рекомендації допоможуть знизити ризики витоку особистих даних і їх слід дотримуватись кожному користувачу мережі Інтернет.

Кіберзлочини мають наслідки не лише для окремих осіб, що стали жертвами, але й для багатьох організацій, компаній, урядів та й для всього суспільства загалом. Найчастіше вони становлять загрозу для життєво важливих сфер суспільства і можуть вчиняти негативний вплив на всі верстви суспільства. Тому кіберзлочинність є загрозою національній безпеці в усьому світі і більшість держав зацікавлені в тому, щоб запобігти витоку персональних даних своїх громадян в мережі, та зменшенні кількості кібератак, які перешкоджають роботу органів державної влади, лікарням, банкам, підприємствам.

Боротьба з кіберзлочинністю вимагає більшої, і ефективнішої міжнародної співпраці, отже виникає необхідність в об’єднанні країн для спільної боротьби

кіберзлочинності в світі. Стрімкий розвиток цифрових технологій, незважаючи на позитивний вплив на всі сфери людського життя, спричинив, також, зростання й поширення кіберзлочинів. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування.

Нині у нашій країні пріоритетними напрямами для розвитку є саме кібербезпека та протидія кіберзлочинності. Тож протидія кіберзлочинності та рівень кібербезпеки на сьогодні є одним із пріоритетних напрямків в політиці країни. Але для комплексної боротьби з цією проблемою потрібні спільні зусилля держави, громадян та міжнародної спільноти. [2]

Список використаної літератури:

1. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. — К. : ВБ «Аванпост-Прим», 2012. — 214 с.

2. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству / Н. Мыщук // Вісник Львівського університету. Серія економічна. — 2014. — Випуск 51. — С. 173-179.

ВИКОРИСТАННЯ КРИПТОПЕРЕТВОРЕНЬ ДЛЯ ЕФЕКТИВНОГО ЗАХИСТУ ДАНИХ

Черних К.Ю.
Київський національний університет технологій та дизайну
Захарова М.В.

Все більше аспектів нашої життєдіяльності залежить від Інтернету, смартфонів та комп'ютерів. Автомобілі обладнано комп'ютерами, які можуть повністю взяти на себе керування транспортом. Комп'ютерні системи проникають у наші будинки та застосовуються для керування домашньою технікою. Банківські, а також медичні дані, зберігаються в цифровому вигляді. Кожна організація чи

підприємство веде бухгалтерію і внутрішні бази даних в електронному вигляді. Це означає, що вся діяльність людини напряму залежить від комп'ютерної мережі.

Зараз найбільш актуальне використання криптографічних методів захисту в інформаційних системах через поширення використання комп'ютерних мереж по яким передаються великі об'єми інформації державного, військового, комерційного та приватного характеру, який не допускає можливість доступу до неї сторонніх осіб.

Шифрування як спосіб захисту даних.

Криптографічні системи мають у своїй основі алгоритми шифрування за допомогою яких і відбувається процес шифрування та дешифрування інформації і поділяються на:

– Симетричні криптосистеми. Це метод в якому для шифрування та дешифрування використовується один і той самий ключ.

– Асиметричні криптосистеми. Для шифрування та дешифрування використовують два різних ключа (відкритий і закрити), які пов'язані між собою математично.

– Хеш-функції. Їх використовують для створення електронно-цифрового підпису. ЕЦП дозволяє автентифікувати електронні документи, підтвердити справжність інформації, або авторство повідомлення.

Проблеми сучасної криптографії.

Не дивлячись на те, що криптографія досить нова наука у неї вже є проблеми, які необхідно вирішувати. До них відносяться:

– Збільшення розміру шифрованих блоків даних та ключів. Швидкі темпи розвитку обчислювальної техніки призводять до збільшення розмірів блоків даних та їх ключів. Наприклад криптосистема RSA побудована на складності вирахування великих простих чисел. На початку 1991 року було розпочато конкурс по розкладанню RSA – чисел на прості множники, тоді для шифрування інформації було достатньо 330 біт. Внаслідок конкурсу дослідникам вдалося розкласти числа

від RSA – 330 до RSA – 768 біт. На даний момент рекомендований об'єм прийнятний для шифрування інформації не менше 4096 біт.

– Ненадійність фундаменту шифрування. В теорії доведено зв'язок між складно обчислювальними задачами та їх аналогами. Це означає, що якщо буде підібрано ключ до однієї криптосистеми, то відкриються і інші так як аналогічні задачі мають однакову або дуже схожу схему.

– Відсутність перспектив. Існують квантові обчислення – ефективна обчислювальна модель, яка заснована на паралелізації обчислювальних процесів за рахунок перетворення початкової інформації, це означає, що можливо одночасно вирахувати значення функції для всіх її аргументів за один її виклик.

Квантові комп'ютери як вирішення та породження проблем кібербезпеки.

Однією з найбільш багатообіцяючих технологій захисту даних сьогодні аналітики називають квантову криптографію. Ця технологія дозволяє забезпечити практично абсолютний захист шифрованих даних від злому. В основі роботи квантової мережі лежить принцип квантового розподілу ключів. Ключ генерується і передається за допомогою фотонів, наведених в квантовий стан. Скопіювати такий ключ не можна. При спробі злому фотони, що передають інформацію, згідно із законом фізики, змінюють свій стан, вносячи помилки в передані дані. Однак в той ж час стрімка еволюція квантових комп'ютерів створює новий виклик перед фахівцями з кібербезпеки. Особливість квантових обчислень дозволяє реалізувати алгоритми, які можуть за порівняно невеликий проміжок часу зламати будь-які паролі засновані на найбільш розповсюджених на сьогоднішній алгоритмах шифрування. Очікується, що до 2027 року квантові комп'ютери дозволять зламувати найбільш стійкий та поширений алгоритм шифрування RSA-2048.

Головна проблема в тому, що квантові комп'ютери мають «квантову перевагу» тобто їх потужність буде перевершувати будь-яку теоретичну потужність звичайних комп'ютерів. Згідно розрахунків для цього необхідний 50-кубітний комп'ютер, на даний момент є комп'ютер потужністю 72 кубіта.

Рішенням проблеми ризику квантового злому існуючих систем криптографії є перехід на інші алгоритми шифрування. Ряд найбільш перспективних алгоритмічних основ для постквантової криптографії:

– Алгоритми гратчастої криптографії: в даний час розроблено близько 10 різних алгоритмів. Дослідження активно тривають;

– багатовимірна криптографія: кілька запропонованих рішень виявилися нестійкими до злому;

– кеш-криптографія.

Висновок.

Наука розвивається разом з ростом можливостей комп'ютерних систем. За останні десятиліття було розроблено чимало універсальних алгоритмів, які дозволяють з високою надійністю зберігати та передавати інформацію. Найпоширеніші з яких:

– симетричні: AES, «Кузнечик», Camellia, Twofish, Blowfish;

– асиметричні: Elgamal, RSA;

– хеш-функції: MD (4, 5, 6), SHA (-1, -2), «Стрибог».

Зараз в криптографії актуальні проблеми ускладнення криптосистем, підвищення стійкості алгоритмів, а також зменшення розмірів блоків даних. Криптографічні дослідження без сумніву є важливим внеском в майбутнє. Чимало вразливостей в розповсюджених криптосистемах пов'язані також з недоліками проектування та реалізації. Поки що нема підстав припускати, що найближчим часом це зміниться, тому на рівні з теоретичними дослідженнями не треба забувати про підвищення кваліфікації фахівців котрі працюють з криптосистемами.

Література:

1. КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВНОЙ ФАКТОР НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ XXI ВЕКА [Електронний ресурс] – Режим доступу до ресурсу: https://cyberrus.com/wp-content/uploads/2014/03/5-12.pdf.

2. 11 Eye Opening Cyber Security Statistics for 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/.

3. Прогноз развития киберугроз и средств защиты информации 2021 [Електронний ресурс] – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Threats_Analysis/2021-Cyber-Threats-and-Information-Security-Forecast.

4. Технологии кибербезопасности: какие решения перспективны и можно ли полностью защититься уже сейчас [Електронний ресурс] – Режим доступу до ресурсу: https://rb.ru/longread/cybersecurity-today/.

5. Криптографічний захист інформації [Електроний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/kriptograficheskaya/.

6. Кибербезопасность: постквантовая криптография [Електронний ресурс] – Режим доступу до ресурсу: http://xn--80aplem.xn--p1ai/analytics/Kiberbezopasnost-postkvantovaa-kriptografia/.

КІБЕРБЕЗПЕКА У СФЕРІ ПОЛІЦІЇ

Звєгінцева А. М.
Дніпропетровського державного університету внутрішніх справ
Рижков Е.В.
м.Дніпро, Україна

В результаті стрімкого розвитку комп'ютерних технологій і їх застосування в різних сферах нашого життя людство увійшло в нову еру інформатизації, коли комп'ютер є необхідним інструментом в самих різних сферах життєдіяльності людини.

Поглиблюється залежність людини і суспільства в цілому, від комп'ютерних та інформаційних систем. Однак злочини, тим чи іншим чином пов'язані з

комп'ютером, обмеження інтересів користувачів і поширення завідомо неправдивої та іншої небезпечної інформації створюють серйозну загрозу безпеці інформаційної системи, а також інтересам держави, правам і свободам громадянина. Таким чином, проблема правового захисту комп'ютерної та інформаційної систем, профілактика і протидія комп'ютерним злочинам стає актуальною для суспільства і держави.

В даний час добре налагоджена розподілена мережа інформаційно-обчислювальних комплексів здатна зіграти таку ж роль в суспільному житті, яку свого часу зіграли електрифікація, телефонізація, радіо і телебачення разом узяті. Яскравим прикладом цього став розвиток глобальної мережі Internet. Вже прийнято говорити про новий виток у розвитку суспільної формації - інформаційному суспільстві.

Будь-яка економічна і політична діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Цілісність сучасного світу як спільноти забезпечується, в основному, за рахунок інтенсивного інформаційного обміну. Призупинення глобальних інформаційних потоків навіть на короткий час здатна привести до не меншу кризи, ніж розрив міждержавних економічних відносин.

Звичайно впровадження в управлінський процес і інші сфери життя суспільства електронно-обчислювальної техніки, без якої зберігання, обробка і використання величезної кількості найрізноманітнішої інформації було б неможливим, принесло неоціненну користь у розвиток науки, техніки та інших галузей знань. Однак вигоди, які можна отримати завдяки використанню цієї техніки, стали використовуватися і в злочинних цілях. Європейський Союз створив орган під назвою «Форум по кіберзлочинності». Безліч країн підписала Конвенцію Ради Європи щодо кіберзлочинності, яка намагається стандартизувати європейські закони, що стосуються злочинності в Інтернеті.

Таким чином, очевидно, що сьогодні однією з найважливіших проблем є потреба підрозділів поліції грамотними комп'ютерними фахівцями. Співробітник

поліції, який працює в областях пов'язаних із захистом секретної службової інформації, розслідуванням комп'ютерних злочинів і т.п. звичайно повинен володіти всіма необхідними навичками. Однак зараз, дуже часто, в цих областях працюють люди, які прийшли після закінчення цивільних ВНЗ, тому одним із пріоритетних напрямків розвитку освіти в МВС є саме освіта фахівців в комп'ютерній сфері.

Література:

1. Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: Підруч. К., 2009.
2. Корченко О. Г. Системи захисту інформації. К., 2004

СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ

Ковиньов О.А.
Київський національний університет технологій та дизайну
Чепинога А.В.

Актуальність теми.

Спостереження за людьми - важлива дослідницька діяльність для забезпечення безпеки. У зв'язку зі зростаючим попитом на безпеку в різних областях, розробка інтелектуальної та ефективної системи спостереження викликала величезний інтерес в останні роки. Більшість існуючих систем спостереження засновані на монокулярних камерах і обмежені фіксованими кутами огляду і, отже, не можуть надати достатню тривимірну інформацію для розпізнавання і відстеження людини.

Країни в усьому світі знають про такі ситуації, і для забезпечення миру і безпеки свого будинку вони намагаються зробити необхідні кроки для запобігання тероризму і захисту від нього. З цієї причини прогрес в розробці і впровадженні технологій відеоспостереження швидко збільшується. У міру розвитку технологія

відеоспостереження перейшла на цифровий записуючий пристрій з використанням технології на основі IP.

Об'єктом дослідження є розпізнавання руху об'єкта в системах відеоспостереження.

Мета роботи: порівняння видів систем відеоспостереження, та використання системи розпізнавання обличчя для забезпечення безпеки на підприємстві.

Наукова новизна:

1. Виконано порівняльний аналіз систем відеоспостереження, які використовують метод розпізнавання рухомих об'єктів. Також визначені ситуації, в яких дані системи будуть корисні, і їх переваги і недоліки.

Як для аналогової, так і для цифрової камери існують додаткові спеціалізовані функції, такі як камери, які можуть записувати якісні зображення при поганому освітленні, камери з декількома напрямками, камери, які можуть знімати зображення з великої відстані, і багато іншого.

Нижче наведені лише деякі з спеціалізованих опцій камери:

Внутрішні / зовнішні купольні камери: антивандальні і найбільш поширені для базового внутрішнього / зовнішнього спостереження, купольні камери не дозволяють зловмисникам дізнатися, в якому напрямку може бути направлена камера.

PTZ-камери (з нахилом, масштабуванням): ці камери дозволяють оператору відеоспостереження або охоронцеві активно переміщати камеру вліво або вправо, вгору або вниз, а також віддаляти або приближати об'єктив.

Непомітні камери: як випливає з їх назви, ці камери погано видно і забезпечують чітке зображення. Вони можуть бути замасковані під різні предмети, можуть бути закріплені або підперті і ідеально підходять для використання всередині приміщень.

Кульові камери: довгі і циліндричні за формою, вони найбільш ефективні для використання на відкритому повітрі, так як забезпечують чітке зображення на великій відстані.

Тепловізійні / інфрачервоні камери: використовуються в багатьох аеропортах, морських портах і приміщеннях, які забезпечують критично важливу інфраструктуру, інфрачервоні камери можуть забезпечувати якісне цілодобове спостереження незалежно від часу доби і якості освітлення. Вони можуть відобразити рухомі фігури навіть в непроглядній темряві, а лінзи мають дальність дії понад 900 футів (274 м).

Камери ANPR/LPR: Камери автоматичного розпізнавання номерних знаків (ANPR) або розпізнавання номерних знаків (LPR) представляють собою вузькоспеціалізовані камери, здатні зчитувати і зберігати дані про номерні знаки .

Камери високої чіткості: забезпечують зображення з таким високим дозволом, що вони в основному використовуються в закладах з дуже високими ризиками, таких як казино і банки.

Розпізнавання облич стало очевидним завдяки розвитку технологій. Ідентифікація осіб при відеоспостереженні завжди була складною областю, де необхідно було пройти ряд досліджень, щоб ідентифікувати конкретну особу на відео. Спочатку виявлення осіб в реальному часі виконується з використанням середовища з відкритим вихідним кодом, який запускається в обробці і пізніше захоплені особи співвідносяться з шаблонними особами, які зберігаються в базі даних, як тільки особи ідентифіковано, відображається профіль людини, щоб повідомити про поведінковому статус людини, який вивчається.

По результатам дослідження видно що, сучасні технології значно розширили можливості систем відеоспостереження. Камери відеоспостереження тепер можуть пропонувати розпізнавання осіб, інтелектуальні камери, такі як PTZ-камери з інтелектуальним відстеженням, яке дозволяє їм ідентифікувати і стежити за людьми або транспортними засобами, поки вони не вийдуть за межі діапазону - тепловізійні

камери, нічне бачення, повнокольорове зображення високої чіткості і різні інтелектуальні технології, які дозволяють камерам негайно відправляти повідомлення про конкретні види діяльності.

Література:

1. WHAT IS A VIDEO SURVEILLANCE SYSTEM? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://blog.koorsen.com/what-is-a-video-surveillance-system#:~:text=A%20video%20surveillance%20system%20%2F%20CCTV,of%20a%20building%20or%20property.
2. Uzialko A. How to Choose a Video Surveillance System for Your Business [Електронний ресурс] / Adam Uzialko. – 2020. – Режим доступу до ресурсу: https://www.businessnewsdaily.com/9067-choosing-a-surveillance-system.html.
3. What Are the Different Types of CCTV Camera [Електронний ресурс] – Режим доступу до ресурсу: https://www.caughtoncamera.net/news/different-types-of-cctv/.
4. Different CCTV camera types and what they offer [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.ifsecglobal.com/video-surveillance/cctv-camera-types-explained/.
5. MOST POPULAR TYPES OF CCTV CAMERAS [Електронний ресурс] – Режим доступу до ресурсу: https://www.caldersecurity.co.uk/most-popular-types-of-cctv-cameras/.
6. Face recognition in surveillance system [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7192887.

ЗАХИСТ WIFI МЕРЕЖІ В СУЧАСНИХ УМОВАХ КІБЕРЗЛОЧИННОСТІ

Гордієнко І.М.
papDeath@gmail.com
Київський національний університет технологій та дизайну
Захарова М.В.

На сьогоднішній день, головною проблемою щодо захисту особистої інформації, постає безпека бездротових мереж. На відміну від особливостей

дротових мереж, які мають повноцінний базис аналізу та пошуку всіх можливих вразливостей, бездротові мережі в аспекті передачі даних (з етапом конвертації інформації) через радіохвилі, мають лише часткові етапи захисту WPA. Даний протокол захисту, а точніше його більш актуальні версії WPA2 (з апгрейдами) та WPA3, стали основоположенням будь яких технологій захисту як на апаратному так і на програмному рівні.

Головною метою даної роботи, постає вивчення та аналіз протоколів захисту WiFi мереж WPA, їх оновлення та вразливості.

Доступ до глобальної мережі, встановлюється через точки доступу, якими в свою чергу виступають роутери на базі технології WiFi. Саме через такий тип підключення, мережу поділяють на два типи, бездротові мережі відкритого та закритого типу. Мережа відкритого типу най вразливіша в даному аспекті, так як повноцінний захист, як правило встановлений лише типовою автентифікацією на віддаленому сервері, а захист по типу підключення пристрою напряму уникають, через громіздкість роботи. Найпростіший варіант крадіжки інформації відбувається наступним чином, потік даних перенаправляється напряму через кіберзлочинця, що дає йому повний доступ, але лише до етапу автентифікації запиту. Мережа закритого типу, встановлює автентифікацію кожного наступного приладу при підключені до мережі, а також має внутрішнє шифрування в каналах передачі даних. В сучасних умовах найпоширенішими технологіями захисту постають WPA2 яке на відміну від свого попередника WEP має комбінований аналіз мережі, та WPA3.

Згідно інформації від компаній по створенню та продажу маршрутизаторів, більшість бюджетних маршрутизаторів має в наявності захист лише типу WPA2 і лише окремі сегменти мають тип шифрування WPA3. WPA2 оновлений тип WPA, отримав інноваційний стандарт шифрування даних AES а також стандарт автентифікації 802.1. Навіть якщо ви використовуєте надійне шифрування, це не означає, що ваша мережа непроникна для атаки. Ваш пароль бездротової мережі (він

же загальнодоступний ключ під WPA2) так само важливий, як і сильне шифрування [**Ошибка! Источник ссылки не найден.**]. Головною вразливістю даного типу по сьогодні залишається внутрішній захист, тобто якщо кіберзлочинець зможе отримати доступ до мережі, то неповноцінність класової ієрархії дає можливість керування даними кожного приладу під'єднаного до мережі.

Не дивлячись на вище сказане, даний тип являється найбільш поширеним і його використання залежить від способу автентифікації, так як він розділений на 2 типи:

WPA2 – Personal (PSK) даний тип, представлений в виді канонічного способу автентицікації, шляхом введення єдиного ключа для всіх пристроїв задля доступу до мережі. Ключ зберігається на кожному з пристроїв окремо задля подальшої можливості перегляду чи заміни по необхідності.

WPA2 – Enterprise даний метод дещо складніший в реалізації, так як його використання можливе лише при наявності RADIUS-server для самостійної видачі паролів, але він забезпечує високий рівень захисту.

WPA3 даний тип був введений в 2018 р як повноцінна заміна WPA2, яка включатиме в себе вирішення основних вразливостей минулих версій та матиме нові поліпшення. Зокрема, буде посилено безпеку навіть якщо користувачі обирають «слабкий» пароль мережі, а також буде спрощено налаштування приладів без дисплеїв. Також буде посилено захист приватних даних користувачів у відкритих мережах шляхом індивідуальних налаштувань алгоритмів шифрування. Нарешті, буде додано підтримку набору 192-бітних криптографічних алгоритмів англ. *Commercial National Security Algorithm* (CNSA) розроблених комітетом з національних систем інформаційної безпеки (англ. *Committee on National Security Systems*)[1].[**Ошибка! Источник ссылки не найден.**] Головним аспектом задля ведення нового протоколу стало вирішення однієї з головних проблем, а саме вразливість KRACK. Виявлена вразливість дозволяє повторно встановлювати один і той самий криптографічний нонс на третьому кроці в

процедурі відкриття сеансу (так зване рукостискання) за протоколом WPA2. Завдяки цьому зловмисник має можливість здійснити криптоаналіз та встановити сеансовий ключ. Таким чином, зловмисник може «прослуховувати» дані, а в деяких випадках, навіть «підробляти» дані, що передаються між клієнтом та точкою доступу.[**Ошибка! Источник ссылки не найден.**]

Так як і WPA2, WPA3 було створено в 2 типах: WPA3 – Personal та WPA3 – Enterprise.

WPA3 – Personal даний тип давав можливість обирати найпростіший пароль, але при цьому зберігати високий рівень захисту.

WPA3 – Enterprise даний тип був створений першочергово для повноцінності безпеки підприємств, який встановлював 192-розрядну систему захисту.

На базі типів WPA2 та WPA3, будується класифікація сучасних маршрутизаторів їх захисна можливість та залежність цінового діапазону.

Таким чином, безпека мережі потребує повноцінної уваги, так як на сьогодні встановлені канони мають невирішені вразливості згідно класової ієрархії та автентифікація користувачів і лише знання про взаємодію системи з користувачем, особливість вразливостей типів захисту та його етапи шифрування, допоможуть більш ретельно зрозуміти, як забезпечити повноцінний потік конфіденційних даних.

Література:

1. WPA2? WEP? Що найкраще шифрувати для захисту мого Wi-Fi? [Електронний ресурс] // 4 meahc. – 2021. – Режим доступу до ресурсу: https://ukr.4meahc.com/wpa2-wep-whats-best-encryption-secure-my-wi-fi-26172.
2. Wi-Fi Protected Access [Електронний ресурс] // ВікіпедіЯ. – 2017. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Wi-Fi_Protected_Access.
3. Security [Електронний ресурс] // WiFi - Alliance. – 2020. – Режим доступу до ресурсу: https://www.wi-fi.org/discover-wi-fi/security.
4. KRACK [Електронний ресурс] // ВікіпедіЯ. – 2017. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/KRACK.

5. How the KRACK attack destroys nearly all Wi-Fi security [Електронний ресурс] // ars TECHNICA. – 2017. – Режим доступу до ресурсу: https://arstechnica.com/information-technology/2017/10/how-the-krack-attack-destroys-nearly-all-wi-fi-security/.
6. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks [Електронний ресурс] // Internet Archive. – 2003. – Режим доступу до ресурсу: http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf.

СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ З ЗАХИСТУ ІНФОРМАЦІЇ

Данілов Д.В.,
ddvdani14@gmail.com
Київський національний університет технологій та дизайну
Захарова М.В.

За минулі півстоліття спостерігався стрімкий ріст в сфері інформаційних систем, зокрема і систем підтримки прийняття рішень. З розвитком інформаційних систем стало зрозуміло, що коли-небудь внесені дані до інформаційних систем можуть передаватися безкінечну кількість разів до того ж безконтрольно. З тих пір питання захисту персональних даних стало одним з найважливіших завдань як приватних так і державних організацій.

Мета даної роботи – визначити особливості використання систем підтримки прийняття рішень для захисту інформації, а саме для покрашення роботи засобів запобігання загрозам.

Однією з найпоширеніших загроз безпеки є помилки допущені персоналом який обслуговує систему. Такі помилки можуть призвести до повної зупинки роботи системи або можуть створити вразливі місця якими в майбутньому можуть скористатися зловмисники. Також поширеними загрозами є комп'ютерні віруси та скоординовані розподілені атаки. До уваги також потрібно брати загрози на які

людина ніяк не може вплинути, такими загрозами можуть бути природні катаклізми, паводки, землетруси тощо.

У 1960-х роках системи підтримки прийняття рішень (СППР) в більшості використовувалися для забезпечення менеджерів структурованими періодичними звітами, а самі СППР базувалися на дуже потужних та дорогих комп'ютерах (мейнфреймах). В той же час створення IBM System 360 а також інших потужних процесорних систем зробило побудову систем управлінської інформації в великих корпораціях більш практичним і економічним.

В 1970-х роках системи підтримки прийняття рішень стали значно складнішими комп'ютерними системами, які підтримували ціноутворення, виробництво, маркетинг, а також, логістичні функції [1].

На початку 1990-х років програмне забезпечення бізнес-аналітики, сховищ даних та OLAP (On-Line Analytical Processing) почали розширювати можливості систем підтримки прийняття рішень.

Приблизно в 1997 році сховище даних стало основою інтеграційного сховища знань, що сприяло більш швидкому і ефективному способу прийняття рішень.

Важливо розуміти, що рішення сама СППР не приймає, рішення приймає оператор системи, який вводить вхідні дані в програму, яка в наступному видає йому можливі варіанти розв'язання проблем.

Існує дуже багато видів систем підтримки прийняття рішень таких як:

● СППР керовані даними (Data driven DSS) – це СППР які фокусуються на доступі до внутрішніх даних компанії, а також коли це потрібно на зовнішні дані, та маніпулюють ними.

● СППР керовані моделями (Model-Driven) – це СППР що керується моделлю, яка може походити з різних дисциплін наприклад: бухгалтерські моделі, моделі оптимізації, фінансові моделі тощо. Такі системи не вимагають великих баз даних адже вони спираються на маніпулювання та доступ до моделі ніж до даних.

● СППР керовані знаннями (Knowledge driven). Такі СППР надають оператору пропозиції та / чи рекомендації засновані на аналізі певної бази знань, це повинно допомогти операторові в прийнятті вірного рішення.

● СППР керовані документами (Document driven). Такі СППР допомагають операторові в керуванні та в отриманні не структурованих документів та веб сторінок, впроваджуючи різні технології для обробки та зберігання, щоб забезпечити аналіз та пошук документів. Система також має доступ до різних документів наприклад: протоколів засідань компанії, політики компанії, корпоративних записів, специфікації продукції, історичних документів компанії, тощо, а також зазвичай для конкретного завдання керується пошуковою системою.

● СППР керовані комунікацією (Communication driven). Такі СППР ще називають груповими тому, що вони використовують моделі прийняття рішень та комунікацію для прийняття вірного рішення операторами, які працюють в групі. Як правило такі СППР підтримують обмін документами, планування та електронну комунікацію для підняття продуктивності, а також прийняття рішень, вони також застосовують такі технології як електронна пошта, двостороннє інтерактивне відео, тощо.

● Внутрішні та міжорганізаційні СППР (Inter- and Intra-organization DSS). Такі системи виникли завдяки стрімкому зростанню Інтернету та інших мережевих технологій: WAN, LAN, тощо. Міжорганізаційні СППР застосовуються для обслуговування клієнтів, постачальників компанії, тощо, в той час як внутрішньоорганізаційні СППР спрямовані на конкретні групи користувачів та людей в компанії.

Отже, в роботі було досліджено типові загрози, та види СППР, які з одного боку можуть бути дуже корисними для різних організацій, а з іншого можуть бути причиною путанини та неточного аналізу тому, що такі системи призначені для прийняття оперативних рішень, а аж ніяк для виявлення «неправильних» рішень, і вся відповідальність за прийняте рішення лежить на операторові системи.

Література:

1. Decision support system - Wikipedia [Електронний ресурс]. — Режим доступу: https://en.wikipedia.org/wiki/Decision_support_system (Дата звернення: 14.03.21).
2. Decision Support Systems Framework with Links [Електронний ресурс]. — Режим доступу: https://dssresources.com/dsstypes/ (Дата звернення: 14.03.21).
3. Online Analytical Processing (OLAP) [Електронний ресурс]. — Режим доступу: http://www.compinfo-center.com/entsys/olap.html (Дата звернення: 14.03.21).
4. A Brief History of Decision Support Systems [Електронний ресурс]. — Режим доступу: https://dssresources.com/history/dsshistory.html (Дата звернення: 14.03.21).
5. Communications Driven and Group Decision Support System [Електронний ресурс]. — Режим доступу: https://www.managementstudyguide.com/decision-support-system-architecture-networking-security-issues.htm (Дата звернення: 14.03.21).

УПРАВЛІННЯ ДОСТУПОМ ДО ОБЛІКОВИХ ЗАПИСІВ КЛІЄНТІВ ІНТЕРНЕТ-ПРОВАЙДЕРА

Ваксютенко І.С.,
Igorkyn2@gmail.com
Київський національний університет технології та дизайну
Захарова М.В.

На сьогоднішній день сфера інформаційних технологій (IT) дуже стрімко розвивається і тим самим несе в собі цінну інформацію. Кіберзлочинці своїми нападами бажають отримати приватні дані користувачів, а саме: документи, паролі, логіни, кошти, тощо. Кожного дня, користувачі використовують різну техніку (ноутбуки, телефони, телевізори, планшети, тощо) для перегляду сайтів в інтернеті, залишаючи певну інформацію про себе. Зазвичай, сайти збирають конфіденційну інформацію непомітно, тим самим не завжди зрозуміло що їм відомо. Відвідуючи будь-яке інтернет посилання, користувач автоматично надає згоду на обробку даних

пристрою, який використовує [1]. Коли користувач проходить реєстрацію на будь-якому сайті він також надає інформацію про себе.

Метою роботи – дослідити можливості взламування облікових записів та знати найефективніші способи захисту інформації користувача. Один із видів безпеки даних це реєстрація користувача на сайті. Переходячи на різні посилання в інтернеті слід пам’ятати, що деякі сайти можуть бути небезпечними, починаючи з спаму та реклам, закінчуючи втратою коштів та особистих даних. Для того щоб безпечно користуватися інтернет-ресурсами, слід пам'ятати правила:

1) Використовувати тільки складні паролі, а саме, комбінація з цифр та букв(великих та маленьких), а також використовувати інші символи.
2) Нікому не повідомляти свої дані для авторизації.
3) Не надавати приватну інформацію про себе і своїх близьких та знайомих в інтернеті.
4) Не поширювати в інтернеті заборонений контент.
5) Не відкривати посилання від третіх осіб та посилання які мають підозрілу назву [3].

Дотримуючись цих простих правил користувач зможе захистити доступ до облікового запису і значно зменшити ризик загрози взлому.

На даний момент сучасні системи захисту паролів є вразливими. Більшість веб-сайтів, на яких ми реєструємось, інформують нас на скільки захищений наш пароль. Також, від сайтів зареєстрованому користувачу приходять сповіщення на електронну скриньку про те, що потрібно змінювати паролі хоча б один раз на декілька місяців. Кожного разу, коли клієнт проходить аутентифікацію на сайті, він вводить дані для входу, зазвичай це логін (ім’я користувача, номер телефону чи Email) та пароль. Аутентифікація - це процедура встановлення належності користувачеві інформації в системі його ідентифікатора. Ця технологія перевірки встановлює контроль доступу системи, перевіряючи, чи збігаються дані що вводить користувач при авторизації синхронізуючи її з обліковою інформацією в базі даних

зареєстрованих користувачів чи на сервері аутентифікації даних сайту. Пароль, який відомий тільки користувачу, має назву фактор аутентифікації знань. Після аутентифікації користувач проходить процес авторизації, щоб зрозуміти, чи має він дозвіл аутентифікованого користувача на доступ до захищеного ресурсу або системи. Користувач може пройти аутентифікацію, але може не мати доступ до ресурсу, якщо користувачеві був заблокований доступ до нього. Терміни аутентифікації та авторизації між собою взаємозамінні. Хоча вони часто використовуються разом, функції які вони виконують, відрізняються. Аутентифікація це перевірка ідентичності зареєстрованого користувача, перед тим, як надати доступ до захищеного ресурсу, авторизація є процесом перевірки інформації, чи отримав авторизований користувач дозвіл на доступ до потрібних йому ресурсів. Контроль доступу - процес, завдяки якого доступ до потрібних ресурсів лімітується обмеженою кількістю користувачів. Аутентифікація користувача відбувається під час взаємодій від людини до пристрою, за допомогою якого користувач працює в мережі, за межами облікових записів гостей, автоматично належать до облікових записів. Як правило, людина повинна вибрати ім'я користувача чи ідентифікатор користувача та надати існуючий пароль щоб розпочати користування системою. Аутентифікація дозволяє користувачам автономно використовувати техніку в операційних системах та додатках, також забезпечує доступ до мережних і підключених до Інтернету систем, ресурсів і програм.

Найбільш поширені рішення питань захисту облікових записів від кібер атак:

- Двофакторна аутентифікація - додає ще один рівень захисту процесу аутентифікації. 2FA потребує, щоб користувач вказав другий фактор аутентифікації окрім пароля.
- Багатофакторна аутентифікація потребує від користувачів аутентифікації більше чим один фактор аутентифікації, включаючи біометричний фактор.

- Одноразовий пароль - це рандомно створений числовий чи буквено-цифровий рядок символів, яка аутентифікує користувача [3]. Цей пароль можна використовувати лише для одноразового входу або транзакції.
- Біометрія - процес перевірки ідентичності користувача за допомогою ваших вимірювань вашого тіла (обличчя, око, палець).
- Мобільна аутентифікація - це процес перевірки людини через їхні пристрої або перевірку самих пристроїв. Процес аутентифікації через мобільний включає багатофакторну аутентифікацію, яка може складатися з одноразового паролю, біометричну аутентифікацію чи QR-коду.
- Аутентифікація API - стандартні методи керування автентифікацією API: HTTP basic autentification; Ключі API та OAuth.
- Відкрита авторизація (OAuth) - це відкритий стандарт для аутентифікації та авторизації на основі маркерів в Інтернеті.

Отже, можна зробити висновки, що будь-яке використання мережі Інтернет є небезпечним. Але, слідуючи ряду правил та застережень можна майже повністю захистити свої дані від кіберзлочинців. В цілях захисту доступу до свого облікового запису потрібно задіяти декілька видів аутентифікації одночасно.

Література:

1. Pressrelease-webauthn [Стаття]: - Режим доступу до ресурсу: https://www.w3.org/2019/03/pressrelease-webauthn-rec.html

2. Yubico’s 2019 State of Password and Authentication Security Behaviors Report [Електронний ресурс]: - Режим доступу до ресурсу: https://www.yubico.com/press-releases/yubicos-2019-state-of-password-and-authentication-security-behaviors-report/

3. Нові стандарти для беспарольної аутентифікації [Електронний ресурс]: - Режим доступу до ресурсу: https://habr.com/1cloud/blog/353966/

4. Cyber Security requires strong UX [Електронний ресурс]: - Режим доступу до ресурсу: https://hackernoon.com/cyber-security-requires-an-important-ingredient-strong-ux-d0727a0c076

5. The challenge on doing good UX [Електронний ресурс]: - Режим доступу до ресурсу: https://uxdesign.cc/the-challenge-on-doing-good-ux-on-cybersecurity-startups-3b747079def1

6. UX design for cybersecurity [Електронний ресурс]: - Режим доступу до ресурсу: https://medium.com/@MatthewDoan/

6. Federated identity managment [Електронний ресурс]: - Режим доступу до ресурсу: https://searchsecurity.techtarget.com/definition/federated-identity-management

8. FIDO U2F [Електронний ресурс]: - Режим доступу до ресурсу: https://www.yubico.com/solutions/fido-u2f/

ОБ'ЄКТ ТА СУБ'ЄКТ КРИМІНАЛЬНОГО АНАЛІЗУ

Ольга Бойко,
курсант 2-го курсу
Факультету підготовки фахівців
для підрозділу кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ
Кисельов Андрій Олександрович
Доцент кафедри
оперативно-розшукової діяльності
Факультет підготовки фахівців
кримінальної поліції
кандидат юридичних наук, доцент
майор поліції

Якщо розглядати кримінальний аналіз у повному обсязі, то кримінальний аналіз — це дії направлені на ідентифікацію та точне визначення взаємозв'язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаними з ними

та даними, що походять з різних джерел і їх використання правоохоронними органами та судами [1].

Отже, головним об'єктом кримінального аналізу є інформація, у тому числі і криміногенного характеру, яка отримується з якомога більшої кількості інформаційних джерел. А також об'єктами кримінального аналізу виступають споживачі інформації, чиї потреби задовольняються під час його проведення та явища і процеси, що відбуваються в сфері службової діяльності Національної поліції (оперативна обстановка, окремі злочини, загрози з боку злочинного середовища, організація розкриття та розслідування злочинів, організація та планування правоохоронної діяльності, тощо).

Звернувши увагу на завдання, які ставляться при проведенні кримінального аналізу ми бачимо, що об'єктами кримінального аналізу є насамперед особи, причетні до злочинної діяльності, злочини та злочинність. Оскільки саме вони підлягають головному дослідженню [2].

При розгляді процесу кримінального аналізу, як системи, суб'єктів кримінального аналізу можна розділити на три основні групи, в залежності від їх відношення до цього процесу:

1.Керівний склад слідчих та оперативних підрозділів Національної поліції, які приймають рішення, та є одними з основних користувачів результатів проведеного кримінального аналізу. Окрім цього саме вони можуть визначати подальші напрямки у разі необхідності проведення додаткових досліджень.

2. Кримінальні аналітики – фахівці, які виконують безпосередні завдання по проведенню кримінального аналізу, саме вони створюють нову інформацію для прийняття управлінських, процесуальних та практичних рішень щодо подальшого розкриття та розслідування злочинів.

3. Працівники слідчих підрозділів та підрозділів кримінальної поліції, які безпосередньо здійснюють організацію розкриття та розслідування злочинів, та потребують і готують завдання на проведення кримінального аналізу в залежності

від наявної інформації, стану роботи за наявними практичними завданнями, рівня наявної інформації, необхідної для подальшого проведення слідчих та оперативно-розшукових дій.

Інформаційна цінність – це властивість, яка встановлюється наявністю можливого впливу на прийняття відповідного рішення. Критерії оцінювання інформації мають базуватися на адекватності завданням, які постають у кожному конкретному випадку та мають стратегічний характер.

Інформація може стосуватися різноманітних галузей. Така інформація має бути не застарілою, адже інформаційний продукт є річчю «швидкопсувною» [3].

Список використаної літератури:

1. Одеський державний університет внутрішніх справ. Посібник з елементами тренінгу. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/149/1/%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BA%D1%80%D1%96%D0%BC.%20%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83%20%281%29.pdf.

2. https://www.slideshare.net/NationalPolice/ss-75925350

3. https://www.naiau.kiev.ua/news/kriminalnij-analiz-u-sistemi-zasobiv-protidiyi-organizovanij-zlochinnosti.html

ІНФОРМАЦІЙНІ РЕСУРСИ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС КРИМІНАЛЬНОГО АНАЛІЗУ

Протасов Сергій Олександрович
здобувач вищої освіти 2 курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ
Кисельов Андрій Олександрович
доцент кафедри оперативно-
розшукової

діяльності факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент,
майор поліції

Вступ. Сьогоднішній ступінь розвитку суспільства характеризується швидким збільшенням потоків та обсягів інформації. Сучасну діяльність органів Національної поліції України досить важко уявити без використання інформаційного забезпечення, інформаційних ресурсів, технологій та баз даних.

Основними тенденціями розвитку інформаційних ресурсів під час здійснення кримінального аналізу являється: удосконалення управління системи інформаційного забезпечення, централізація та інтеграція інформаційних даних, впровадження сучасних інформаційних технологій, використання спеціальних засобів захисту інформаційних ресурсів, налагодження обміну кримінальною інформацією на міждержавному рівні.

Використання та вимоги до інформаційних ресурсів, які використовуються під час здійснення кримінального аналізу досліджували такі вчені: І.В. Арістова, О.М. Бандурка, К.І. Бєлякова, Р.А. Калюжний, М.Я. Швець, Є.Б. Кубк, В.А. Кормич, В.С. Цимбалюк, В.Д. Гавловський та ін..

На протязі останнього часу проблема забезпечення інформаційними ресурсами для здійснення кримінального аналізу привернула увагу таких науковців, як В.Я. Мацюка, О.В. Олійника, Д.Я. Семир'янова, О.В. Сирового, Д.В. Сулацького та інших вчених, але великий перелік питань у даній галузі ще очікує на свою наукову розробку.

Мета. На підставі аналізу наукової літератури та вітчизняного законодавства розкрити сутність інформаційного забезпечення, яке необхідно для здійснення кримінального аналізу.

Матеріали та методи. Матеріали дослідження – Кримінальний Кодекс України, нормативно – правові акти, праці вітчизняних та зарубіжних вчених. Методи дослідження – діалектичний, компаративний, формально-логічний, системний, логічного узагальнення, поділу понять та системного аналізу.

Результати та обговорення. Кримінальним аналізом являється мисленнєво-аналітична робота працівників правоохоронних органів, яка полягає в перевірці і оцінюванні інформаційних ресурсів, їх інтерпретації, встановленні зв'язку серед даних, які отримуються під час розслідування і мають значення для кримінального провадження для того, щоб їх використали правоохоронні органи і суд в подальшому проведення оперативного та стратегічного аналізу [4, с.15].

За своїм характером, кримінальний аналіз може бути загальним та спеціалізованим. Кримінальний аналіз загального характеру має направлення на велику частку злочинних діянь, звичайно у галузі невеликих відомств чи юрисдикцій. Спеціалізований кримінальний аналіз має призначення для певних типів злочинної діяльності чи об'єктів, наприклад наркотики, промислове шпигунство чи організована злочинність.

Кримінальний аналіз характеризується тактичним та стратегічним застосуванням. Тактичний кримінальний аналіз направлений на короткострокові завдання правоохоронних органів чи кримінальні провадження, що безпосередньо розслідується. За даним аналізом передбачаються негайні дії, тобто затримання особи, накладення арешту, вилучення предметів чи документів тощо [4, с.16].

Стратегічний кримінальний аналіз використовується щодо вирішення більш широких довгострокових проблем та задач, наприклад, для виявлення крупних фігур злочинного світу чи синдикатів, прогнозу збільшення видів злочинної діяльності та встановлення пріоритетів діяльності правоохоронних органів [2, с.48].

Інформаційними ресурсами, які використовуються під час здійснення кримінального аналізу можуть бути матеріали з різноманітних джерел, таких як спостереження, звіту, чуток та інших джерел. Інформаційні ресурси можуть бути як

правдивими так і помилковими, достовірними чи недостовірними, підтвердженими чи непідтвердженими, актуальними чи неактуальними [5, с.114].

Інформаційною цінністю являється властивість, що встановлює наявність можливий вплив на прийняття відповідного рішення. Критерії оцінки інформаційних ресурсів мають підґрунтя на адекватності завдань, що постають у кожних конкретних випадках і характеризуються стратегічним характером. Загальними критеріями даного оцінювання виступають [1, с.104]:

- Актуальність. Інформаційні ресурси можуть стосуватися різних галузей. Такий інформаційний ресурс може бути не застарілим тому, що інформаційний продукт являється річчю «швидкопсувною».

- Важливість. Інформаційні ресурси повинні відповідати критерію важливості тому, що вони являються релевантними, змістовними, тобто є відповідними завданням, має зв'язок з стратегічними напрямками діяльності. Важливість інформаційного ресурсу може визначатися за 3 категоріями [3, с.65]:

а) відомості, на які необхідно негайно відреагувати;

б) відомості, на які не потрібно негайно відреагувати, але вони мають суттєве значення щодо подальшого прийняття стратегічного рішення;

в) відомості, на які на даний час відсутній безпосередній вплив щодо прийняття рішень, але їм властивий довідковий характер та за належного підходу вони можуть бути використані щодо вирішення проміжного завдання.

- Достовірність. Достовірність є критерієм, що здійснює визначення об’єктивності інформаційного ресурсу, тобто його відповідність дійсності. Даний факт визначається за принципом верифікації, тобто осмислення можливостей його існування взагалі. Достовірність інформації має залежність від надійності джерел здобутого інформаційного ресурсу.

- Корисність. За даним критерієм визначається прийнятність інформаційного ресурсу щодо вирішення конкретного завдання. Стає явним, що

отримані інформаційні ресурси можуть мати довідковий, загальний характер. Але дане узагальнення завжди відноситься до головного об'єкту впровадження.

- Своєчасність. Інформаційні ресурси повинні бути корисними саме у теперішній момент, якщо вони потребують негайного реагування.

- Повнота. За даним критерієм можна визначити наскільки інформаційні ресурси з'ясовують і описують проблеми, події або явища. Цей критерій здійснює окреслення, чи було встановлено вичерпну низку складових, наявність яких являється достатньою у прийнятті відповідних рішень.

- Безперервність. Інформаційні ресурси не може бути дискретними, разовими. Висвітлення того або іншого процесу чи події повинно носити постійний, безперервний характер.

- Прогностичність. Являється комплексним критерієм. За даним критерієм передбачається властивість інформаційного ресурси в сприянні визначення ймовірної тенденцій і перспектив розвитку ситуації. Прогнозування поділяється на [6, с.57]:

а) прогнозування, як імовірнісні твердження щодо майбутніх подій і процесів з відносно великим відсотком ймовірності;

б) передбачення, як самоочевидне (не імовірнісне) твердження щодо майбутніх подій і процесів, що мають основу на абсолютній достовірності;

в) антиципації, як логічно сконструйована модель майбутнього з до сих пір не визначеним відсотком імовірності;

г) сценарії, що не можуть передбачити майбутнє, а тільки формують його можливі варіанти.

Інформаційні ресурси можуть бути: відкриті і приховані, зі різних джерел, в тому числі з правоохоронних та інших відомств та осіб. Інформаційними ресурсами можуть бути [7, с.135]:

Конфіденційний інформатор: особа з безпосереднім доступом до інформації, яка має відношення до незаконних форм роботи та систем, що надають дану інформацію правоохоронним органам.

Інформаційні ресурси добуті за допомогою здійснення операції під прикриттям, тобто сплановане впровадження співробітників або співробітника в злочинну групу, злочинну організацію чи їх інфраструктуру для того щоб отримати певний елемент інформації щодо системи.

Інформаційні ресурси добуті за допомогою попереднього розслідування тобто висновки, що були виконанні на підстав попереднього збору та аналізу інформації щодо відповідних заходів боротьби з кримінальною діяльністю, організаціями та особами.

Інформаційні ресурси добуті за допомогою правових інструментів: використання даних інструментів як арешт та повістка в суд щодо отримання інформації із захищених джерел чи осіб, які відмовляються від співпраці.

Інформаційні ресурси добуті з системи зберігання та отримання інформації: використання даних, що вже зібрані та зберігаються в сховищах даних, таких як картотека чи комп'ютерна база даних.

Речові докази тобто інформація щодо фізичного положення, отримана з місця злочину, про жертву, про підозрювані особи та їх оточення.

Аудіо, відео контроль осіб тобто здійснення таємного спостереження за діяльністю осіб чи особи.

Технічне спостереження тобто приховане спостереження за діяльністю та фіксація із використанням технічних засобів.

Взаємний обмін, тобто інформація, що отримана чи обмінена з іншими правоохоронними органами.

Регіональні мережі «кримінальної розвідки», тобто агентства за обміном інформації, що надають певні послуги з підтримкою в конкретних регіонах;

Відкриті джерела, тобто використання інформації, яка вже зібрана державними відомствами та іншими установами, у тому числі і дані держустанов;

Відкриті посилання, тобто наукові роботи та інші джерела, наприклад газети, журнали, ЗМІ, Інтернет.

Інтерв'ю, тобто інформація, отримана за допомогою використовування запланованого, але неформального діалогу, при цьому учасники інтерв'ю не відносяться один до одного з ворожістю.

Дебріфінг є офіційною сесією питань та відповідей серед членів того ж підрозділу, агентства чи професії.

Також криміналісти під час здійснення кримінального аналізу накопичують свої великі бази даних. В даних базах може міститися інформація стосовно правопорушень та кримінальних подій; правопорушників та злочинців; викрадених та вилучених речових доказів, власників мото та автотранспортних засобів; вогнепальної зброї, осіб, які розшукуються та безвісти пропавши та інша інформація.

Висновки. Отже, під час здійснення кримінального аналізу використовуються наступні інформаційні ресурси: конфіденційні інформатори, інформаційні ресурси добуті методом здійснення операцій під прикриттям, добуті методом попереднього розслідування; добуті методом правових інструментів; добуті з системи по зберіганню та отриманню інформації; речові докази, аудіо та відеоконтроль особи, технічне спостереження, взаємний обмін інформацією, регіональні мережі «кримінальної розвідки», відкриті джерела та посилання, інтерв'ю, допит, дебріфінг та накопичені бази даних криміналістів.

Список використаних джерел:

1. Захаров В.П. Сучасні методики аналітичної роботи в сфері оперативно-розшукової діяльності ОВС / В.П. Захаров, В.Ю. Журавльов // Вісник Львів. держ. ун-ту внутр. справ. 2017. № 2. С. 103-115.

2. Мукоіда Р.В. Розвиток системи кримінального аналізу у структурах правоохоронних органів України / Р.В. Мукоіда // Кримінальна розвідка: методологія, законодавство, зарубіжний досвід: матеріали Міжнародної науково-практичної конференції (м. Одеса, 29 квітня 2016 р.). Одеса: ОДУВС, 2016. С. 48-50.

3. Никифорчук Д.Й. Проведення аналізу оперативно-розшукової інформації: монографія / Д.Й. Никифорчук, О.Ю. Бусол. К., 2010. 165 с.

4. Основи кримінального аналізу : посіб. з елементами тренінгу / Користін О. Є., С. В. Албул, А. В. Холостенко та ін. Одеса : ОДУВС, 2016. 112 с.

5. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і начальному процесі: збірник наукових статей за матеріалами доповіді Всеукраїнської науково-практичної конференції 23 грудня 2016 р. / упоряд. Т.В. Магеровська. Львів: ЛьвДУВС, 2017. 313 с.

6. Санакоєв Д.Б. Аналітична обробка інформації в системі кримінальної розвідки оперативних підрозділів кримінальної поліції / Д.Б. Санакоєв // Кримінальна розвідка: методологія, законодавство, зарубіжний досвід: матеріали Міжнародної науково-практичної конференції (м. Одеса, 29 квітня 2016 р.). Одеса: ОДУВС, 2016. С. 57-58.

7. Сегірьова Т.Л. Інформаційні технології в діяльності правоохоронних органів та необхідність їх вивчення курсантами вищих навчальних закладів системи МВС. Вісник Луганського національного університету ім.. Т.Шевченка. 2011. №15. 335 с.

КРИМІНАЛЬНИЙ АНАЛІЗ – ЦЕ ЕФЕКТИВНА РОБОТА ПОЛІЦІЇ ТА БЕЗПЕКА ГРОМАДЯН

Карасьов О.А
Міністерство внутрішніх справ
Дніпропетровський державний
університет
внутрішніх справ

Кафедра оперативно-розшукової діяльності
Доцент Кісєльов А.О
м. Дніпро, Україна

Для того, щоб розглядати дану тему, нам потрібно насамперед потрібно зрозуміти та вивести точне поняття, що ж таке кримінальний аналіз в структурі правоохоронних органів.

За своєю сутністю кримінальний аналіз – це мисленнево-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленню зв'язків між даними, що отримуються у процесі розслідування та мають значення, для кримінального провадження з метою їх використання правоохоронними органами.

Застосування кримінального аналізу впідрозділах Національної поліції підвищує відповідальність розкриття тяжкого та особливо тяжкого злочину.

Для чого існує підрозділ аналітики Національної поліції. В першу чергу - для розкриття злочинів, також він орієнтований на проведення оперативного, тактичного та стратегічного аналізу.

Оперативний аналіз – це опрацювання матеріалів кримінального провадження, метою якого є створення та перевірка фактів, які міг вчинити злочинець, також можливо встановити чи є вірогідність злочинної групи, ролі її членів під час підготовки та вчинення злочинів.

Тактичний кримінальний аналіз – це націлені задачі для правоохоронців, які безпосередньо розслідуються. Тактичний аналіз – допомагає тактично правильно спланувати негайні дії з боку правоохоронних органів:

- Затримання осіб;
- Накладання арешту;
- Вилучення предметів або документів в затриманих особах.

Стратегічний аналіз – це стратегії в розслідуванні злочинів, згідно правилам операції. Також, він спрямований на аналіз діяльності злочинних груп.

Хочемо наголосити, що якісна робота працівників поліції – це завжди безпека громадян. Кожна людина, не важливо з якої вона країни, якої вона національності, віросповідання – потребує безпеки, не залежно від її місцезнаходження, проживання. Тому, не залежно від підрозділу поліції, відбираються тільки ті працівники, які пройшли навчання. І наша країна, дає нам можливість проходити це навчання із залученням експертів європейських країн, так само і в оперативно – аналітичному підрозділі. В цих країнах досить давно існують такі підрозділи, тому нам є чим в них навчатися, взяти до уваги, зрозуміти.

Кримінальний аналіз – це ефективна робота поліції та безпека громадян, який містить в собі методи, які ми хочемо перечислити:

1. Збирання матеріалу для аналізу, оцінки, реалізації інформації для розкриття злочинів

2. Розроблення тактичних та стратегічних засад для протидії злочинців, які ми раніше вказували.

Далі ми розберемо типи аналітичних продуктів.

Перший найпоширеніший – аналітичний звіт, що включає в себе огляд та з'ясування всіх обставин:

- Пошук та відбирання інформації із зовнішніх та внутрішніх джерел;
- Аналіз отриманої інформації;
- Надання аналітичних рекомендацій

Наступним є профіль особи, який представляє собою детальну інформацію, щодо особи злочинця.

Також існує інформаційне зведення – оброблені дані шляхом вибору їх з бази даних за критеріями ініціатора.

Аналіз думок кримінологів, криміналістів, які досліджують проблеми

криміналістичного, кримінологічного прогнозування, та вчених у галузі оперативно-розшукової діяльності дозволяє надати типовий формалізований

алгоритм оперативно-розшукового прогнозування як складової кримінального аналізу, який, на наш погляд, повинен складатися з таких етапів:

- формулювання мети і завдань прогнозу;

- аналіз результатів оперативно-розшукового моніторингу, негативні та позитивні чинники, що впливають на стан оперативної обстановки;

- систематизація, перевірка з використанням альтернативних джерел (ЗМІ, державні та суспільні установи, опитування громадян, соціологічний моніторинг) та аналіз зібраної інформації;

- оцінка існуючого на конкретному об`єкті оперативної уваги та в цілому в державі (залежно від ієрархічного положення оперативного підрозділу) стану оперативної обстановки щодо попередження злочинності;

- визначення чинників, що впливають на стан оперативної обстановки, їх позитивного та негативного впливу;

- побудова математичної моделі оперативної обстановки;

- отримання вихідних даних щодо прогнозу;

- розробка альтернатив розвитку оперативно-розшукової ситуації залежно від вибору варіанта моделі організації ОРД;

- розробка узагальнюючого прогнозу.

Аналогічно прогноз може здійснюватися відповідно до поведінки осіб зі злочинного середовища тощо. При цьому прогнозування може бути:

- для планування та проведення окремого заходу та оперативнорозшукової операції;

- короткострокове – квартал, півріччя, рік;

- середньострокове – п`ять-десять років;

- довгострокове – п`ятнадцять та більше років.

Таким чином, оперативно-розшукове прогнозування повинно розглядатися як невід'ємна частина процесу оперативно-розшукового моніторингу у складі кримінального аналізу та бути його результативною частиною.

Винберга вимагають, що означені види кримінального аналізу повинні бути засновані на сучасному програмному забезпеченні та відповідному рівні комп'ютерної техніки.

Список використаних джерел:

1. Власюк О. В. Використання кримінального аналізу в оперативно-розшуковій діяльності / О. В. Власюк // Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. – 2012. – № 6. – С. 82–85.

2. Гринчак Я. В. Деякі аспекти використання кримінального аналізу в діяльності правоохоронних органів країн Європи та США / Я. В. Гринчак // Центрально- український правничий часопис Кіровоград. юрид. ін.-ту ХНУВС. – 2010. – Спец. вип. – С. 268–273.

3. Махнюк А. В. Теоретичні основи провадження кримінального аналізу у сфері правоохоронної діяльності / А. В. Махнюк // Науковий вісник Державної прикордонної служби України. – 2011. – № 4. – С. 3–7.

4. Власюк О. В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України / О. В. Власюк // Матеріали постійно-діючого науково-практичного семінару. – Харків : Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого. – 2011. – Вип. № 3. – Ч. 1. – С. 82–85.

5. Дем'янчук О. І. Практика застосування оперативно-розшуковими підрозділами Західного регіонального управління кримінального аналізу у сфері протидії незаконній міграції на державному кордоні України / О. І. Дем'янчук, Ю. М. Ковбаса, М. І. Сідор // Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. – 2010. – № 2. – С. 76–83.

6. Козлов Д. В. Використання в оперативно-розшуковій діяльності можливостей кримінального аналізу на морській ділянці відповідальності / Д. В.

Козлов // Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. – 2011. – № 5. – С. 48–53.

7. Треус А. С. Стан запровадження системи кримінального аналізу в оперативнорозшукових підрозділах Державної прикордонної служби України / А. С. Треус // Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. – 2009. – № 1. – С. 53–59.

8. Фаріон О.Б. Алгоритм проведення стратегічного кримінального аналізу оперативно-розшуковими підрозділами державної прикордонної служби України / О.Б. Фаріон // Сучасні інформаційні технології у сфері безпеки та оборони. – № 3 (15). – 2012. – С. 106–110.

МЕТОДИ ПРОВЕДЕННЯ АУДИТУ КІБЕРБЕЗПЕКИ

Вакуленко А.С.
Черкаський державний бізнес-коледж
Захарова М.В.

На даний моменту великій кількості компаній є певний досвід організації інформаційної безпеки. Однак відділ банківських та фінансових послуг є найбільш привабливим для кібератак та кібершахрайства через можливість отримання зловмисниками значних фінансових та нефінансових вигід. Тому проводять визначення та усунення недоліків систем, якими можуть користуватися шахраї для кібератак. Перед проведенням якісного аудиту, необхідно визначити вимоги та процедури аудиту, що включають перевірки операційних систем. Крім того, необхідно ретельно планувати та погоджувати всі процедури аудиту, щоб звести до мінімуму ризик переривання інформаційних систем компанії.

Метою роботи є визначення методів, за допомогою яких можна проводити аудит інформаційної безпеки. Аудит інформаційної безпеки — це дослідження стану захищеності інформаційної системи з точки зору незалежного висококваліфікованого консультанта в області інформаційних технологій, який надає оцінку поточного стану системи інформаційної безпеки, що встановлює

рівень її відповідності певним критеріям, а також результати у вигляді рекомендацій. Крім того, аудит інформаційної безпеки повинен бути системним процесом отримання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки.

Аудит можна розділити на два види:

· зовнішній аудит;

· внутрішній аудит.

Зовнішній аудит — це, як правило, разовий захід, що проводиться за ініціативою керівництва організації або акціонерів.

Внутрішній аудит проводять штатні працівники, для перевірки, оцінювання та моніторингу відповідності й функціювання інформаційних систем.

Аудит безпеки інформаційних систем є невід'ємною частиною системи інформаційної безпеки на підприємстві. Цілями проведення аудиту безпеки є:

· аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів інформаційної системи;

· оцінка поточного рівня захищеності інформаційної системи;

· визначення проблемних місць в системі захисту інформаційної системи;

· визначення та оцінка відповідності інформаційної системи; існуючим стандартам в області інформаційної безпеки;

· розробка рекомендацій щодо підвищення рівня захищеності та ефективності систем і механізмів захисту інформаційної системи;

· розробка політик безпеки та інших організаційно-правових документів з інформаційної безпеки

· впровадженні розроблених документів в роботу організації;

· розробка рекомендацій по навчанню і безпосереднє навчання користувачів і обслугового персоналу інформаційної системи; з питань забезпечення інформаційної безпеки;

· розгляд, вивчення і визначення причин інцидентів, пов'язаних з порушення

інформаційної безпеки, і розробка методів щодо недопущення подібних інцидентів у майбутньому.

Аудит планується з урахуванням статусу та важливості процесів і зон, що підлягають перевірці, а також результатів попередніх аудитів. Повинні бути визначені критерії, область, періодичність та методи проведення аудиту. Відбір аудиторів і процедура аудиту повинні забезпечувати його об'єктивність і неупередженість. Аудитори не повинні проводити перевірку своєї власної роботи.

Висновок. У зв'язку з тим що, в цей час більшість компаній забезпечують інформаційну безпеку на недостатньому рівні та одночасно з цим, не мають доступних і простих методів проведення аудиту інформаційної безпеки, існує потреба в запропонованих стандартом, методів проведення аудиту, а також дійсних сторонніх методик для визначення найбільш ефективних та простих методів проведення аудиту інформаційної безпеки.

Література:

1. ДСТУ ISO / IEC 27001-2005. Інформаційна технологія. Методи і засоби забезпечення безпеки. Системи менеджменту інформаційної безпеки вимоги

2. Аудит інформаційної безпеки: [Електронний ресурс]: Аудит інформаційної безпеки. Аналіз захищеності систем і додатків // URL: https://www.pentestit.ru/audit/

3. Аудит безпеки інформаційних систем - ISO27000.ru: [Електронний ресурс]: Аудит безпеки інформаційних систем // URL: http://iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/audit-bezopasnosti informacionnyh-sistem

СИСТЕМА ДЛЯ ЗАХИСТУ ПОВІДОМЛЕНЬ СПІВРОБІТНИКІВ ОРГАНІЗАЦІЇ

Гринін І.В.
igor.grynin98@gmail.com
Київський Національний університет технологій та дизайну
Захарова М.В.

Співробітники є найбільшим надбанням будь-якої організації. Але відсутність спілкування може змусити персонал відчувати себе невпевненим і не

обізнаним, що шкодить моральному духу компанії. Коли персонал не повідомляється про критичні події, він може розчаруватися або погіршити ситуацію.

Співробітники заслуговують на те, щоб їх повідомлення були захищені від протиправних дій інших сторонніх осіб. Задоволеність роботою та безпека залежать від ефективного передавання відповідної інформації.

Для підвищення захищеності даних співробітників необхідно виконати п'ять основних кроків, які організації повинні зробити, щоб не публічна інформація залишалася приватною. Крім того, організації повинні встановлювати та застосовувати політику захисту інформації, яка допоможе їм дотримуватися правил конфіденційності:

Крок 1: Визначте та визначте пріоритет конфіденційної інформації

Крок 2: Вивчіть поточні потоки інформації та проведіть оцінку ризиків

Крок 3: Визначте відповідні політики доступу, використання та розповсюдження інформації

Крок 4: Впровадити систему моніторингу та забезпечення

Крок 5: Періодично переглядайте прогрес

Таким чином, захист конфіденційних інформаційних активів на всьому підприємстві це серйозна проблема, яку потрібно вирішувати. Це принципово вимагає систематичного виявлення конфіденційних даних; розуміти поточні бізнес-процеси; розробляти відповідні політики доступу, використання та розповсюдження; і контролювати вихідні та внутрішні комунікації. Зрештою, найважливішим є розуміння потенційних витрат та наслідків не створення системи захисту не публічної інформації зсередини.

Список використаних джерел:

1. Harison J. Key messages for employers, employees and OSH personnel [Електронний ресурс] / Jon Harison. – 2014. – Режим доступу до ресурсу: https://www.commerce.wa.gov.au/worksafe/key-messages-employers-employees-and-osh-personnel.

2. Is the employer allowed to read an employee's e-mail [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://tietosuoja.fi/en/is-the-employer-allowed-to-read-an-employee-s-e-mail.

3. 10 cybersecurity best practices that every employee should know [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html.

4. PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

5. Засоби та методи захисту інформації [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://buklib.net/books/28625/.

6. Захист від витоку інформації [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: http://integritysys.com.ua/security/dlp/.

ПРОБЛЕМИ ВПРОВАДЖЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В ОРГАНАХ ТА ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Андрій Щур,
курсант 2-го курсу Факультету підготовки фахівців для підрозділу кримінальної поліції Дніпропетровського державного університету внутрішніх справ
Кисельов Андрій
Доцент кафедри ОРД ФПФПКП Майор поліції кандидат юридичних наук Дніпропетровського державного університету внутрішніх справ

Вступ. Проблема впровадження новітніх методик кримінального аналізу в діяльності Національної поліції України являється досить актуальною. Рівень злочинності має тенденцію до зростання, особливо в галузях корупції та економіки, то і вимагає від органів Національної поліції використання нових навичок щодо організації протидії злочинності, нових підходів для здійснення більш корисного

опрацювання правоохоронними працівниками інформаційних ресурсів, що має повинно мати підгрунття на системному аналізі різних даних, що відносяться до вирішення задач оперативно-розшукової діяльності. Найважливішу роль у даному питанні покладене на здійснення кримінального аналізу інформаційних ресурсів, які отримані працівниками правоохоронних органів.

На основі застосування різнопланових даних, у першу чергу оперативно-розшукових інформаційних ресурсів, кримінальний аналіз дає можливість щодо встановлення індивідуальної чи групової приналежність різних об'єктів оперативної уваги підрозділів Національної поліції; здійснювати дослідження їх властивостей і стану, результатів та співвідношення різних чинників, які можуть на них певним чином здійснювати вплив; здійснювати прогноз щодо подальшого ходу кримінальних подій; виявляти приховані взаємозв'язки серед об'єктів тощо.

Дослідженням питань щодо використання кримінального аналізу в діяльності в підрозділах правоохоронних органах займалися наступні науковці: О.В. Власюк, Я. В. Гринчак, А. В. Махнюк, О. І. Дем'янчук, Ю. М. Ковбаса, Д. В. Козлов, М. І. Сідор, А. С. Треус, О.Б. Фаріон.

Але на даних час в зазначених дослідженнях не розглядався перелік низка проблем, що пов'язані з основними викликами сьогодення до поліції - перебудова моделі роботи Національної поліції з реактивної на проактивну. Зазначене в умовах існування інформаційного суспільства потребує постійної аналітичної роботи та пошуку на основі реструктуризації та оптимізації інформаційних інформації. Підгрунтям зазначеного являється кримінальний аналіз. І як наслідок, потрібно здійснити його адаптацію до вимог сьогодення.

Мета. На підставі аналізу наукової літератури та вітчизняного законодавства дослідити проблеми впровадження кримінального аналізу в органах та підрозділах Національної поліції.

Матеріали та методи. Матеріали дослідження – Кримінальний Кодекс України, нормативно – правові акти, праці вітчизняних та зарубіжних вчених.

Методи дослідження – діалектичний, компаративний, формально-логічний, системний, логічного узагальнення, поділу понять та системного аналізу.

Результати та обговорення.

Кримінальний аналіз - це дії, які мають спрямування на ідентифікацію та точне визначення взаємозв'язків серед відомостей, що відносяться до подій, які мають злочинний характер, осіб, що є пов'язаними з ними і даними, які надходять з різноманітних джерел, та в майбутньому їх використання слідчими органами, прокуратурою і судами [1, с.82].

До загальної мети кримінального аналізу відноситься напрацювання нових напрямів в оперативно-розшуковій роботі і досудовому розслідуванні кримінальних проваджень; для того, щоб отримати детальний аналіз продукту щодо об'єктів кримінального аналізу; якісне планування окремих оперативно-розшукових заходів і слідчих (гласних і негласних) дій; аналітичне супроводження оперативно-розшукової роботи і досудового розслідування; аналіз стану і показників ефективності досудового розслідування, оперативно-розшукової і превентивної роботи щодо протидії злочинності; обробку великих обсягів інформації, що здійснюють унеможливування відстежити і пов'язати факти без використання спеціальних методів аналізу; аналіз складної та розгалуженої структури зв'язків об'єктів оперативно-розшукової роботи чи кримінального провадження; виявлення ризиків, майбутніх тенденцій розвитку злочинності та, в майбутньому, її запобігання; вирішення великих довгострокових проблем та завдань для того, щоб виявити крупні фігури злочинного світу чи синдикатів, прогноз збільшення видів злочинної діяльності та встановлення напрямків роботи правоохоронних органів; аналіз інформаційних ресурсів, які спрямовані щодо виявлення тенденцій, закономірностей, прогнозу розвитку на великий часовий проміжок [2, с.3].

На основі використання різних відомостей, у першочерговому порядку оперативно-розшукові інформаційні ресурси, кримінальний аналіз дає можливість щодо встановлення індивідуальної чи групової приналежності різноманітних

об’єктів оперативної уваги підрозділів кримінальної поліції; здійснювати дослідження їх властивостей і стану, результати та співвідношення різноманітних чинників, які можуть здійснювати на них певний вплив; здійснювати прогноз подальшого ходу кримінальних подій; здійснювати виявлення прихованих взаємозв’язків серед об’єктів тощо.

Безсумнівно, для щоб здійснити розв’язання поставлених задач перед оперативними органами кримінальної поліції досить великий ступінь відіграє ефективність роботи спеціалізованих підрозділів Управління кримінального аналізу, що був створений в 2017 році.

Але, на сьогодні практично жоден суб’єкт правоохоронної діяльності не зміг здійснити формування досить ефективної системи інформаційно-аналітичних підрозділів, яка базується на підставі створення єдиного інформаційного простору свого відомства, вже не кажучи про питання інтеграції в даному напрямку всіх органів та підрозділів Національної поліції.

На даний час не був створений єдиний підхід [3, с.162]:

1) щодо питань створення інформаційної бази аналітичної діяльності, що розуміє під собою здійснення ефективної реєстрації кримінально активних осіб, кримінальних подій та фактів, сформування оперативно-розшукового обліку і інтегрованого банку даних оперативно-розшукового призначення;

2) щодо питань процесу автоматизації аналітичної діяльності з урахуванням використання можливостей інформаційних, лінгвістичних та комп’ютерних технологій.

Також до проблем впровадження кримінального аналізу в роботу правоохоронних органів відносять [4, с.55]:

відсутність концепції про впровадження кримінального аналізу в роботу правоохоронних органів;

відсутність сучасної нормативно-правової бази у галузі формування і використання моделі кримінального аналізу в діяльності правоохоронних органів;

є не на належному рівні використання можливостей кримінального аналізу в структурних департаментах правоохоронних органів;

недостатній рівень забезпечення оперативних підрозділів правоохоронних органів сучасною оргтехнікою та відповідним комп'ютерним програмним забезпеченням;

відсутність системи навчання, підготовки і перепідготовки працівників аналітичних підрозділів згідно з світовою моделлю поліцейської діяльності;

відсутність сучасних методик збору і обробки інформаційних ресурсів з «вулиці» згідно з стандартами ЄС 4*4/ 5*5; формування відповідних інформаційних баз даних тощо.

До недавнього часу все, що було зв'язано з аналізом та прогнозом, мало підгрунття в основному на положеннях, які були розроблені криміналістичною наукою. Але на сьогодні, створилася потреба в розробці та подальшому використанні принципово нових комплексних аналітичних підходів та методів, що розраховані на швидко змінювані оперативні обставини, в фундаменті яких закладено не лише криміналістичні знання, а й знання з інших наукових галузей.

На сучасному етапі аналітична діяльність являється одним з основних елементів процесу пізнання, що здійснюється під час вирішення задач оперативно-розшукової роботи та оволодіння оперативними працівниками кримінальної поліції початковими методиками в проведенні кримінального аналізу тільки дасть позитивний вплив на показники якості протидії злочинності.

Звісно ж, складові кримінального аналізу інформаційних ресурсів прямо чи побічно є присутніми в всіх галузях оперативно-розшукової роботи. Отже, зміст кримінального аналізу потрібно досліджувати у більш ширших аспектах – не лише як вид діяльності спеціалізованих суб'єктів в галузі інформаційно-аналітичного забезпечення оперативних підрозділів кримінальної поліції, але й у вигляді органічної оперативно-розшукової функції, до впровадження якої є причетними всі діючі оперативні працівники.

Отже, визначивши основні проблеми впровадження кримінального аналізу в діяльність правоохоронних органів наведемо шляхи подолання зазначених проблем [4, с.58]:

1) прийняти на рівнях МВС і НП України перспективну концепцію щодо формування моделі поліцейської діяльності, як основу використання кримінального аналізу в роботі всіх структурних підрозділів Національної поліції.

2) розробити і прийняти відомчі і міжвідомчі інструкції, що мають спрямування на створення організаційно-технологічної моделі поліцейської роботи, кримінального аналізу в органах Національної поліції і аналітичної підтримки органів досудового розслідування.

3) розробити національне експертне програмне забезпечення аналітичних підрозділів для того, щоб здійснювати аналіз одержаної в процесі аналітичного пошуку інформаційних ресурсів.

4) розробити і впровадити програмне забезпечення для того, щоб провести тактичний аналіз в рамках конкретних кримінальних проваджень, а також забезпечити формування слідчих версій. Наведені програми потрібно внести до стандартів підготовки слідчих органів досудового розслідування.

5) створити на основі ВНЗ факультету підготовки фахівців аналітичних підрозділів і введення окремих дисциплін за темою «Використання інформаційних технологій для того, щоб виявити і розслідувати кримінальні правопорушення» для факультетів підготовки фахівців для підрозділів кримінальної поліції і органів досудового розслідування.

Висновки. Нами були визначені основні проблеми впровадження кримінального аналізу в діяльність правоохоронних органів та наведені рекомендації щодо подолання даних проблем, це відсутність системи інформаційно-аналітичних підрозділів, концепції, нормативно-правового забезпечення, відповідного програмного та технологічного забезпечення, системи навчання, підготовки та перепідготовки працівників відповідних аналітичних підрозділів,

відсутність сучасної методики щодо збору та обробки інформації з «вулиці» відповідно до міжнародних стандартів, системи формування відповідних інформаційних банків даних тощо. Рекомендаціями щодо подолання вище зазначених проблем можуть бути: прийняття перспективної концепції формування моделі поліцейської діяльності; розробка та прийняття відомчих та міжвідомчих інструкцій, впровадження програмного забезпечення; створення на базі одного з ВНЗ факультету підготовки фахівців для аналітичних підрозділів та введення окремих відповідних дисциплін.

Список використаних джерел:

1. Власюк О. В. Використання кримінального аналізу в оперативно розшуковій діяльності / О. В. Власюк // Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. 2012. № 6. С. 82–85.

2. Махнюк А. В. Теоретичні основи провадження кримінального аналізу у сфері правоохоронної діяльності / А. В. Махнюк // Науковий вісник Державної прикордонної служби України. 2011. № 4. С. 3–7.

3. Сучасні проблеми правового, економічного та соціального розвитку держави : тези доп. Міжнар. наук.-практ. конф. (м. Харків, 30 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Консультат. місія Європейського Союзу. Харків, 2018.362 с.

4. Треус А. С. Стан запровадження системи кримінального аналізу в оперативно-розшукових підрозділах Державної прикордонної служби України / А. С. Треус // Бюлетень Департаменту оперативної діяльності Адміністрації Державної прикордонної служби України. 2019. № 1. С. 53–59.

РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Корягіна А.К.
kimlina301@gmail.com
Дніпропетровський державний університет внутрішніх справ
Кисельов Ф.О.
доцент кафедри оперативно-розшукової діяльності факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент, майор поліції

На сьогодні кримінальний аналіз в підрозділах Національної поліції України більш частіше почав використовуватись ніж декілька років потому оскільки саме сьогодні більшість інформації про людину можна знайти в мережі Інтернет, чим і користуються підрозділи Національної поліції України в своїй діяльності, такі як кримінальна поліція, патрульна поліція, слідчі підрозділи поліції (Органи досудового розслідування), поліція охорони, поліція особливого призначення, КОРД, поліція превенції, кібер поліція та інші.

Хочеться зазначити що дії кримінального аналізу направлені на ідентифікацію і точне визначення взаємозв’язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаних з ними, та даними, що походять з різних джерел, і їх використання правоохоронними органами і судами, та іншими підрозділами внутрішніх справ. [1, с.3]

Існують декілька виді кримінального аналізу такі як: тактичний, оперативний та стратегічний. Функція тактичного аналізу полягає у встановлені тенденцій злочинності, встановлені місця концентрації вчинення кримінальних правопорушень, встановлення профілю підозрюваного та потерпілого. А ось

оперативний аналіз виконує функції кримінальних проваджень відносно певних осіб, ОПГ, з цілю перевірки тих чи інших гіпотез щодо їх ймовірних злочинної діяльності, встановлення зв'язків тобто основним завданням оперативного аналізу є аналіз в'язків, аналіз телефонних дзвінків, аналіз маршруті, аналіз подій, аналіз потоків та порівняльний аналіз справ. Стратегічний аналіз у свою чергу спрямовується на виявлення такого як тенденцій, закономірностей та прогнозуванню розвитку за певний або за великий проміжок часу тобто це стратегічні управлінські рішення та визначення ризиків розвитку криміногенної ситуації.[2, с.3]

Також існують окремі підрозділи кримінального аналізу в системі Національної поліції України – це Підрозділ кримінального аналізу ДІПКП «102», 2. ІПКП «102» регіональних органів, 3. Підрозділ оперативного та превентивного блоків.

Тобто можна зробити висновок з вище переліченого що Кримінальний аналіз надає підрозділам національної поліції інформацію стосовно кримінальних правопорушень та відомості стосовно осіб, ОПГ та інших злочинних угрупувань стосовно яких мається оперативний інтерес підрозділами внутрішніх справ України.

Література:

1. Користін О.Є., Албул А.В Навчальй посібник « ОСНОВИ КРИМІНАЛЬНОГО АНАЛІЗУ» URL: http://dspace.oduvs.edu.ua/bitstream/123456789/149/1/%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%BA%D1%80%D1%96%D0%BC.%20%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83%20%281%29.pdf

2. Навчальний концепція «Кримінальний аналіз у діяльності поліції» URL: https://www.slideshare.net/NationalPolice/ss-75925350.

Наукове електронне видання

ЗБІРКА НАУКОВИХ ПРАЦЬ

XIII Всеукраїнська
студентська науково-практична конференція
студентів, аспірантів та молодих вчених

за тематикою
«Тенденції розвитку IT-технологій в Україні»

ISBN 777-777-7777-77-7

(електронне видання)

Матеріали XIII Всеукраїнської
студентської науково-практичної конференції
студентів, аспірантів та молодих вчених

Комп'ютерна верстка: *к.т.н., Бурмістров С.В.*
Відповідальний за випуск: *к.т.н., Хотунов В.І.*
Дизайн обкладинки:*Оліфіренко В.М.*