Державний університет телекомунікацій

IV МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ»

ЗБІРНИК ТЕЗ

20-21 грудня 2017 року

м. Київ

State University of Telecommunications

IV INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "ACTUAL PROBLEMS OF INFORMATION AND CYBERNETIC SECURITY"

BOOK OF ABSTRACTS

December 20-21, 2017

Kyiv

УДК 621.387:681.327

Актуальні проблеми забезпечення інформаційної та кібернетичної безпеки Матеріали третьої міжнародної науково-технічної конференції. Збірник тез. — Київ : ДУТ, 2017. — 53 с.

Даний збірник містить тези учасників конференції, представлених на IV МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ», яка проводилась 20-21 грудня 2017 р. в Навчально-науковому інституті Захисту інформації Державного університету телекомунікацій, м. Київ.

Робочі мови конференції - українська, російська, англійська.

Секретарі конференції

Киричок Р.В. асистент кафедри Інформаційної та кібернетичної безпеки, Державний університет телекомунікацій.

Платоненко А.В. ст. викладач кафедри Систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій.

Рабчун Д.І. асистент кафедри Кафедра Управління інформаційної та кібернетичної безпекою, Державний університет телекомунікацій.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Програмний комітет:

ДОВБЕШКО Станіслав Володимирович *(к.т.н., доцент. , Київ, Україна);*
ВИШНІВСЬКИЙ Віктор Вікторович *(д.т.н., проф., Київ, Україна);*
КИРИЧОК Роман Васильович (*асистент, Київ, Україна);*
ОКСІЮК Олександр Глібович *(д.т.н., доцент, Київ, Україна);*
САМОХВАЛОВ Юрій Якович *(д.т.н., проф., Київ, Україна);*
ЮДІН Олександр Костянтинович *(д.т.н., проф., Київ, Україна);*
КОРЧЕНКО Олександр Григорович *(д.т.н., проф., Київ, Україна);*
СУБАЧ Ігор Юрійович *(д.т.н., доцент, Київ, Україна);*
ГОРБЕНКО Іван Дмитрович *(д.т.н., проф., Харків, Україна);*
ДУДИКЕВИЧ Валерій Богданович *(д.т.н., проф., Львів, Україна);*
НАЗАРКЕВИЧ Марія Андріївна *(д.т.н., проф., Львів, Україна);*
ГРИЩУК Руслан Валентинович *(д.т.н., с.н.с., .Житомир, Україна);*

ЗМІСТ

Пазинін А. С.
студент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій
м. Київ, Україна

УРАЗЛИВІСТЬ ANDROID СМАРТФОНІВ

Безсумнівно Android сьогодні є найпоширенішою в світі мобільною системою. Функціональність сучасного смартфона становлять браузери, клієнтські програми соціальних мереж, офісні додатки і всілякі сервіси, що працюють в Мережі. Android-пристрої зайняли більшу частину ринку смартфонів за рахунок відкритої архітектури платформи Android і зручного API розробника. Але, як і будь-яка інша система, Android, на жаль, не може бути цілком безпечною, так як розробники ніколи не зможуть створити ідеальний код. А популярність платформи привертає все більше зловмисників готових використовувати уразливості системи в корисних цілях. На даний момент Android є найбільш популярної мобільної ОС з часткою ринку більше 75%.

В даній тезі я опишу уразливість Android системи, яка ґрунтується на зшиванні корисного навантаження з APK файлом. Кожен пристрій на платформі Android має систему перевірки сертифікату при встановленні нового додатку, але як часті при встановленні нового APK фалу ви читаєте дозволи які йому надаються?

Дослідники Технологічного інституту Джорджії і Каліфорнійського університету в Санта-Барбарі виявили серйозну уразливість, що зачіпає всі версії ОС Android (в тому числі останню версію Android 7.1.2 Nougat). Проблема отримала назву Cloak and Dagger. З її допомогою зловмисник може викрасти інформацію яка зберігається на пристрої, створивши шкідливий додаток, що подає на запит всього два дозволи. Додатку досить лише отримати доступ до BIND ACCESSIBILITY SERVICE ("a11y") і SYSTEM ALERT WINDOW (малювання поверх інших вікон), і воно зможе записувати натиснення на клавіатурі і викрадати паролі і інші конфіденційні дані. Для отримання більш широкого доступу використовується утиліта Msfvenom в дистрибутиві kali linux. Яка є комбінацією утиліт Msfpayload і Msfencode, що об'єднала в собі обидва інструменту в одну платформу Framework instance під назвою msfvenom payload. Файл з шкідливим кодом вшивається в додаток який не викликає підозри у користувача. Що може бути доставлений на смартфон жертви через файлобмінники, соціальні мережі.

Google вжила відповідних заходів щодо поліпшення безпеки своєї мобільної ОС відразу ж після отримання повідомлення про уразливість. «Ми оновили Google Play Protect (наш сервіс безпеки для всіх Android-пристроїв з Google Play) для виявлення і запобігання установки подібних додатків», - повідомили в компанії. Але підтримка сучасних нових моделей смартфонів відбувається не відразу і займає час, що вже казати про не флагманські моделі смартфонів.

Коровайченко Ю. Ю.
студент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій
м. Київ, Україна

ПРОБЛЕМИ ТА РЕКОМЕНДАЦІЇ ЩОДО РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

1) Інциденти кібербезпеки.
2) Типи інцидентів кібербезпеки.
3) Порівняння різних типів інцидентів кібербезпеки.
4) Типові фази в атаці кібербезпеки.
5) Основні проблеми реагування на інциденти кібербезпеки.
6) Рекомендації щодо реагування на інциденти кібербезпеки.

Література

1. Крісі Д. Cyber Security Incident Response Guide / Джейсон Крісі., 2013. – 56 р. – (CREST).

2. Murdoch D. Blue Team Handbook: Incident Response Edition / Don Murdoch.. – (Paperback).

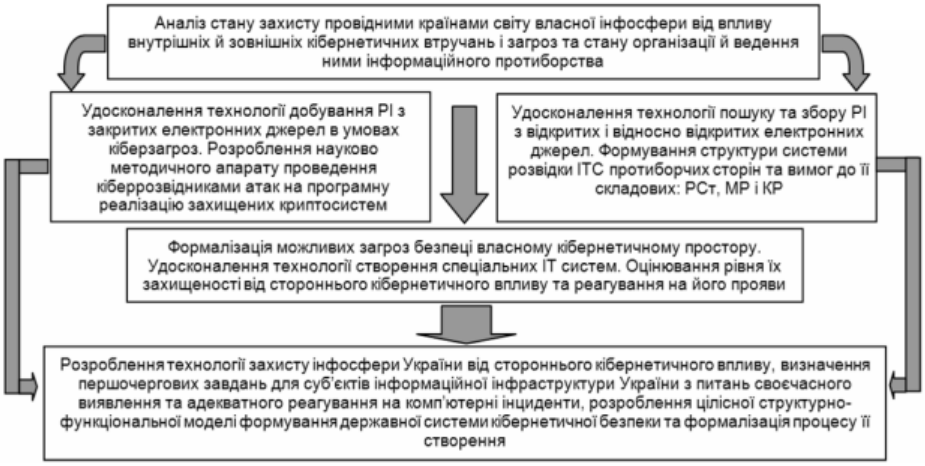
Дорошенко Д. В., Вакуленко А. В.
студенти кафедри Систем інформаційного то кібернетичного захисту інформації
Державний Університет телекомунікацій
м.Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Протидія реальним загрозам та мінімізація потенційних загроз потребує низки кроків держави в ключових сферах життєдіяльності, що мають особливе значення для забезпечення кібернетичної безпеки. З цією метою, держава, у партнерстві з суспільством, недержавним та приватним сектором, з метою посилення кібербезпеки України, буде керуватись такими пріоритетами:

- у зовнішньополітичній сфері;
- у сфері державної та внутрішньополітичної безпеки;
- у воєнній сфері;
- у соціальній, гуманітарній та науково-технологічній сферах.

Одними з першочергових заходів на шляху побудови системи кібербезпеки держави є вдосконалення державного управління у даній сфері та впорядкування нормативно-правового поля. Метою забезпечення кібернетичної безпеки України, має бути створено цілісну Національну систему кібернетичної безпеки. Ключовими завданнями якої має бути: формування та реалізація державної політики в сфері кібернетичної безпеки; моніторинг кібернетичного простору з метою своєчасного виявлення, запобігання і нейтралізації кібернетичних загроз; виявлення, попередження та припинення кібернетичних злочинів. *Варіант структурно-функціональної моделі програми державної системи кібербезпеки:*



Підсумовуючи викладене, можна констатувати, що розуміння сутності організаційного забезпечення системи кібернетичної безпеки України, дозволить суттєво підвищити рівень стійкості такої системи, та забезпечити належний рівень захисту інтересів людини, суспільства, держави у кібернетичному просторі.

Література

1. ГСТУ СУІБ 2.0/ISO/IES 27002:2010 — Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою.

Склярський А. С.
студент кафедри Телекомунікаційних систем і мереж
Державний університет телекомунікацій
м. Київ, Україна

БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Забезпечення захисту інформації в телекомунікаційних мережах вимагає виконання таких завдань: формування і поступове впровадження законодавчої та нормативно-правової бази технічного та криптографічного захисту інформації, гармонізованої з європейськими та міжнародними стандартами; розроблення сучасних методів захисту інформації для забезпечення комплексного захисту інформації в телекомунікаційних мережах; створення системи легального перехоплення інформації з телекомунікаційних мереж у випадках, передбачених законодавством України; створення державного координаційного центру з питань безпеки в інформаційно-телекомунікаційних мережах загального користування, сприяння створенню державних та недержавних центрів компетенції та реагування на інциденти в телекомунікаційних мережах.

Захист інформації передбачається у стратегічно важливих системах оперативно-технічного управління телекомунікаційними мережами та системі управління транспортними магістральними телекомунікаційними мережами. Крім того, має забезпечуватись захист від несанкціонованого втручання в режим функціонування обладнання мереж, а також вирішення проблеми «непрозорості» впроваджуваних в телекомунікаційних мережах іноземних технічних засобів, програмних продуктів і технологій.

Нові проблеми інформаційної безпеки є порівняно складними і мають охоплювати декілька рівнів та сфер діяльності: мережне адміністрування, фізичну безпеку, моніторинг, програмне забезпечення телекомунікацій, інструменти забезпечення безпеки, аудит безпеки.

Поперешняк С.В.
к.ф.-м.н., доц. кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна
Соколенко П.Ю.
студентка кафедри Інженерії програмного забезпечення
Навчально-науковий інститут комп'ютерних інформаційних технологій
Національний авіаційний університет
м. Київ, Україна

ПЕРЕВАГИ ПРОТОКОЛУ IPV6 В INTERNET OF EVERYTHING

Будь-який пристрій, будь то комп'ютер, мобільний телефон або КПК, при підключенні до Інтернету має отримати унікальний числовий ідентифікатор, названий IP-адресою. Рядові користувачі Інтернету практично не стикаються з IP-адресами завдяки існуванню системи доменних імен (DNS). Якщо людина хоче зайти на сайт, він просто вводить його доменне ім'я, не замислюючись про цифри. Однак саме числові IP-адреси лежать в основі функціонування Всесвітньої павутини.

Формат IP-адреси визначено в IP-протоколі, основна функція якого - передача даних через набір об'єднаних комп'ютерних мереж. Вибір шляху передачі даних називається маршрутизацією.

Широко відомий протокол IPv4, створений в 70-і роки минулого століття. Кожен IP-адреса в ньому складається з 32 біт і представлений у вигляді чотирьох чисел по 8 біт, між якими ставлять крапку. Такий підхід дозволяє отримати понад чотири мільярди унікальних IP-адрес. На зорі ери Інтернету здавалося, що цього більш ніж достатньо. А тому адреси цілими блоками видавалися безпосередньо організаціям, серед яких переважали наукові установи та університети.

Пізніше з'явилася нова технологія, яка отримала назву IPv6 або Internet Protocol version 6. В IPv6 довжина IP-адреси розширена до 128 біт, тому число доступних ідентифікаторів збільшується практично до безкінечності.

Таким чином, застосування цієї технології дозволяє забезпечити кожен пристрій, що має доступ в Інтернет, унікальною IP-адресою. А це забезпечує безпосередню взаємодію всіх пристроїв, підключених до Мережі. Така взаємодія дасть можливість, наприклад, управляти кондиціонером, що знаходяться у вас вдома, прямо з офісу. Крім збільшення адресного простору протокол володіє і іншими перевагами. Наприклад, в IPv6 існує окремий тип адрес "anycast address", який дозволяє пристрою, підключеного до Інтернету, відправляти запит будь-якій групі серверів. Це дає можливість вузлу визначити сервер, що знаходиться до нього ближче інших і далі взаємодіяти тільки з ним.

IPv6 розглядається як природна заміна нашої поточної схеми адресації IPv4, оскільки вона спрямована на скорочення падіння та пропонує підвищену функціональність, що може зменшити витрати та підвищити ефективність. Оновлений протокол лежить в основі IoE (Internet of Everything).

Було виділено наступні причини, які говорять нам про важливість IPv6 у Internet of Everything:

1. Безпека

Кожен день створюються мільярди нових смарт-продуктів, і безпека є одним з найважливіших аспектів. IoE висуває цілком нову порцію складних проблем безпеки. Якщо хтось з поганими намірами захоче зламати розумне місто або околиці розумних будинків, результат може бути катастрофічним.

З одного боку, IPv6 може запускати повноцінне шифрування. Шифрування та перевірку цілісності, що використовуються в поточних віртуальних приватних мережах (VPN), є стандартним компонентом у IPv6, доступними для всіх з'єднань і підтримуються всіма сумісними пристроями та системами.

IPv6 також підтримує більш безпечне розпізнавання імен. Протокол Secure Neighbor Discovery (SEND) дозволяє ввімкнути криптографічне підтвердження того, що хост - це той, на який він претендує на момент підключення. І хоча IPv6 не є заміною для перевірки додатків або службових рівнів, вона як і раніше забезпечує підвищений рівень довіри до з'єднань.

2. Масштабованість

З огляду на швидке поширення IoE, з’являється потреба у великій кількості нових адрес, тому легко зрозуміти, чому адреси IPv6 важливі для пристроїв IoE. Творці продуктів IoE, які підключені через TCP/IP, можуть бути впевнені, що для їх пристроїв доведеться зберігати унікальний ідентифікатор протягом тривалого часу.

3. Зв'язність

З IPv4 було багато проблем, що дозволяють IoE-продуктам говорити один з одним. Network Address Translation(NAT) вирішує одну з цих основних проблем. NAT був створений як спосіб вирішення проблем для організацій, яким потрібні численні люди та пристрої, щоб мати можливість працювати з однією адресою IPv4. Це не лише створює проблему безпеки, а й також ставить складну проблему для продуктів IoE. IPv6 дозволяє унікальним чином адресувати продукти IoE. Більші просунуті хост-пристрої мають різного роду інструменти, що полегшують роботу з брандмауерами та маршрутизаторами NAT.

Таким чином, можна сказати що IPv6 це відмінне і необхідне оновлення IPv4, яке відіграє доволі велике значення для Internet of Everything.

Література

1. From Machine-to-Machine to the Internet of Things. Introduction to a New Age of Intelligence., 2006. [Электронный ресурс]. – Режим доступу до ресурса: http://www.mforum.ru/news/article/110233.htm

2. What the Internet of Everything really is – a deep dive. [Электронный ресурс]. – Режим доступу до ресурса: https://www.i-scoop.eu/internet-of-things-guide/internet-of-everything/

Поперешняк С.В.
к.ф.-м.н., доц. кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
Педаш Ю.В.
студентка кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

ОБГРУНТУВАННЯ ВИБОРУ АРХІТЕКТУРИ ДОДАТКУ НА ПРИКЛАДІ МОДЕЛІ ЗАСОБУ ТАЙМ-МЕНЕДЖМЕНТУ

Вибір архітектури програмного додатку – це завжди дуже відповідальний крок. Саме від цього залежить, наскільки програму буде легко та швидко розробляти, підтримувати, модифікувати та покращувати.

Для даного планувальника була обрана реалізація у вигляді веб-застосунку, тому вибір архітектури буде враховувати цей фактор. Веб-додаток – це клієнт-серверний додаток, в якому клієнтом виступає браузер, а сервером – веб-сервер. Логіка веб-додатку розподілена між сервером і клієнтом. Зберігання даних здійснюється, переважно, на сервері. Обмін інформацією відбувається за допомогою мережі.

В результаті аналізу багатьох шаблонів архітектур для веб-застосунків для реалізації цього додатку був обраний архітектурний шаблон MVC.

Архітектура MVC (Model-View-Controller) – це архітектурний шаблон, який поділяє програму на три взаємопов’язані частини: модель, представлення та контролер. Метою цього архітектурного шаблону є відокремлення внутрішнього зображення інформації від способів подання інформації користувачеві та отримання інформації від користувача.

Розглянемо основні терміни, що використовуються в архітектурі MVC. Модель представляє дані в програмі та змінює свій стан в залежності від дій користувача. Зазвичай під моделлю розуміють внутрішні класи програми, що представляють реальні сутності Наприклад, у даному додатку моделлю можуть бути такі класи як «User», «WeekDay», «Event», що містимуть важливі поля з інформацією про сутність та бізнес-методи. Головна ціль представлення в архітектурі MVC – це відображення даних для користувача. У нашому додатку це будуть html та css файли, що міститимуть розмітку та стилі веб-сторінки. Контролер має інтерпретувати дії користувача та тим самим викликати зміни у моделі та представленні.

Розглянемо ці поняття на прикладі. Користувач знаходиться на сторінці «Events» планувальника, де він бачe перелік різноманітних подій у своєму місті, які він може додавати до свого особистого календаря. Він бачить подію, що його зацікавила, та нажимає на кнопку «Add to my Calendar». У цей самий час контролер інтерпретує дії користувача: перевіряє, чи є в його календарі вільне місце в саме цей час і, якщо місце є, додає у базу даних новий рядок про

те, що тепер у користувача в календарі є ця подія. Представлення оновлюється та у своєму планувальнику користувач бачить нову подію.

Переваги архітектури MVC:

- Можлива одночасна розробка додатку - кілька розробників можуть працювати одночасно на моделі, контролері та переглядах.
- Висока єдність - MVC дозволяє разом логічно групувати пов'язані дії на контролері. Представлення на конкретну модель також згруповані разом.
- Слабка зв'язність компонентів - сама природа структури MVC така, що між моделями, переглядами або контролерами існує слабкий зв'язок, тому один можна змінювати без впливу на інший.
- Простота модифікації - через відокремлення відповідальностей моделі, контролера та представлення, майбутня розробка чи модифікація дається набагато легше.
- Кілька представлень для однієї моделі - моделі можуть мати кілька представлень. Дублювання коду в MVC зменшуються до мінімуму, оскільки цей шаблон відокремлює дані та бізнес-логіку від відображення у користувача.

Недоліки архтіектури MVC:

- Архітектура додатку стає складнішою, оскільки програма може використовувати інші шаблони одночасно з MVC.
- Представлення і контролер тісно пов'язані, тобто якщо відбувається модифікація одного з них, це впливає на інший.
- Зміни в інтерфейсі моделі вимагатимуть змін у контролері та перегляді.
- Якщо модель активно використовується, часті зміни моделі можуть призвести до надмірного оновлення відповідних переглядів.
- Розробник серверної частини застосунку має бути обізнаним в тому, як влаштована клієнтська сторона та навпаки.

Отже, незважаючи на деякі недоліки, архітектурний шаблон MVC є досить ефективним та зручним для розробки інтернет застосунку. Він забезпечує слабку зв’язність компонентів, дозволяє швидко модифікувати програму та мати кілька представлень для однієї моделі. Модифікації в одній моделі не впливають на інші.

Література

1. S. Popereshnyak The method of data exchanging between smartphone and smart watch/ S. Popereshnyak, O. Suprun // Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017 14th International Conference. – 2017. – С. 392-395

2. С.В. Поперешняк Аналіз засобів створення слабкозв’язаних компонентів програмного забезпечення // East European Scientific Journal. № 4. – Т. 5. – 2016. – p. 60-66.

Поперешняк С.В.
к.ф.-м.н., доц. кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
Приступа О. І.
студентка кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

ЗАСІБ ДЛЯ ЗАПАМ'ЯТОВУВАННЯ, ЗАСНОВАНИЙ НА СИСТЕМІ ЛЕЙТНЕРА

У сучасному світі щодня до нас надходять гігантські обсяги інформації і кожному з нас потрібно відділяти необхідне від інформаційного шуму, щоб витрачати менше часу на процес отримання нових знань, упорядковувати матеріал заради більшої продуктивності, раціонально розподіляти розумові навантаження, тому все більше набувають популярності альтернативні методики навчання і запам'ятовування.

Яка користь від альтернативних методик? Треба відбирати, впорядковувати, зберігати, запам'ятовувати все більше інформації за коротші проміжки часу, щоб бути конкуренто спроможним, ефективно здобувати знання і йти в ногу з часом. І людському мозку важко ідеально виконувати всі ці функції. Тому має бути спеціальний інструмент, що оброблював би необхідну інформацію, а користувачу залишалось би тільки запам'ятовування. І саме адаптивне навчання найкраще підходить на цю роль.

Що таке адаптивне навчання? Адаптивне навчання передусім пов'язане з комп'ютерними та/або онлайновими освітніми системами, які модифікують презентацію матеріалу для кращого розуміння. До адаптивного навчання відносяться техніки електронного, персоналізованого, мікро- навчання, гейміфікації, візуалізації. Уявіть собі, що кожен користувач може створювати свій власний персоналізований навчальний модуль, спеціально розроблений під їх сильні і слабкі сторони, цілі та інтереси. Більше того, такі підходи не тільки спрощують процес навчання, але і популяризують освіту.

Флеш картки. Основою автоматизованої системи було обрано флеш картки, оскільки вони зручні у використанні, можуть містити у собі невеликі обсяги інформації, мають просту структуру (2 сторони: питання - відповідь, слово – переклад і т.д.), можуть містити графічні, аудіо дані, для форматування змісту можуть використовуватись різні засоби стилізації тексту.

Що таке активне пригадування? В автоматизовану навчальну систему, що розробляється, закладено принцип активного пригадування. Це процес, в якому частина інформації активно витягується з пам'яті на відміну від пасивного перегляду. Наприклад, використовуючи пасивний огляд можна було б прочитати певний факт, і на цьому усе, інформація переходить у короткотривалу память. У активному пригадуванні доведеться витягнути цю інформацію з пам'яті. Якщо людина правильно відповідає, то стабільність її

пам'яті збільшується, факт переходить у довготривалу память, і тому ймовірність пригадування в майбутньому буде більшою.

Суть системи Лейтнера. Методом обробки флеш карток було обрано систему Лейтнера. Вона базується на принципі інтервальних повторень, де періоди повтору карток збільшуються.

У цьому методі картки сортуються по групах залежно від успішності засвоєння інформації на кожній картці. Якщо відповідь з картки згадується користувачем, то картка перекладається в наступну групу. Якщо ж ні, то картка повертається в першу групу. Кожна наступна група повторюється через більший інтервал. Даний метод найкраще підходить для вивчення іноземних мов і медичних термінів.

Веб-сайт. Внаслідок росту популярності веб-технологій в останні роки, для реалізації системи було обрано подання у вигляді сайту. Дане рішення надає можливість перегляду, створення і збереження флеш карток на будь-якому пристрої (ПК, планшет, смартфон) в будь-якому місці з Інтернет покриттям. Також даний вибір сприяє зручному обміну інформацією між користувачами системи і надає фундамент для створення потужної мережі для самоосвіти.

Інструменти розробки. При розробці системи будуть використовуватись технології Node.js і Sequelize.

Node.js — платформа з відкритим кодом для виконання високопродуктивних мережевих застосунків, написаних мовою JavaScript. Призначена не тільки для створення серверних скриптів для веб, а і для створення звичайних клієнтських і серверних мережевих програм. Зручна для обробки великої кількості паралельних запитів завдяки асинхронній моделі запуску коду, заснованій на обробці подій в неблокуючому режимі та визначенні обробників зворотніх викликів.

Sequelize – ORM для Node.js. ORM - технологія програмування, яка зв'язує бази даних з концепціями об'єктно-орієнтованих мов програмування, і тим самим надає можливість зручного доступу до даних, не створюючи надлишкових SQL запитів до баз даних. Вона підтримує діалекти PostgreSQL, MySQL, MariaDB, SQLite і MSSQL, що забезпечує розширюваність програмного забезпечення, а також надає надійну підтримку транзакцій, зв’язків, реплікації.

Отже, буде створена система адаптивного навчання на основі флеш карток з такими функціями: створення флеш карток, редагування, групування в колоди, форматування змісту, вкладення медіа файлів, створення налаштувань для колод, обмін колодами між користувачами системи. Для реалізації моделі буде розроблений веб-застосунок на мові JavaScript з використанням технологій Node.js та Sequelize.

Література

1. С.В. Поперешняк Проблеми підготовки ІТ-спеціалістів // Системи обробки інформації. № 7. – 2010. – С. 127-131

Поперешняк С.В.
к.ф.-м.н., доц. кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
Зозуля І. С.
студентка кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

АВТОМАТИЗОВАНІ КАТАЛОГИ ДОКУМЕНТІВ – УДОСКОНАЛЕНА ФОРМА ДОКУМЕНТООБІГУ НА ПІДПРИЄМСТВІ

На сьогоднішній день важливим є доступ до інформаційних ресурсів і скорочення часових витрат на розв'язання задач пов'язаних з документообігом. Саме електронний документообіг відкриває можливості для удосконалення, довготривалого збереження документів, управління електронним архівом, враховуючи процедури списання та знищення документів. Розробки програм для поліпшення документообігу активно здійснюються як українськими і російськими, так і закордонними компаніями, що безперечно доводить актуальність досліджуваного питання.

Метою роботи є дослідження можливостей автоматизації документообігу й створення каталогів документів та розробка рекомендацій щодо оптимізації процесів автоматизації каталогізації.

Об'єктом дослідження став процес документообігу на сучасному етапі розвитку. Предмет дослідження становлять процеси автоматизації документообігу, зокрема автоматичні процеси створення каталогів документів.

І. Аспекти впровадження автоматизованих систем документообігу

1. Особливості електронного документообігу

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України (254к/96-ВР), Цивільним кодексом України, законами України "Про інформацію", "Про захист інформації в автоматизованих системах" (80/94-ВР), "Про державну таємницю", "Про зв'язок" (160/95-ВР), "Про обов'язковий примірник документів", "Про Національний архівний фонд та архівні установи", а також іншими нормативно-правовими актами.

Державне регулювання електронного документообігу Кабінет Міністрів України та інші органи виконавчої влади в межах повноважень, визначених законом, реалізують державну політику електронного документообігу.

2. Запровадження єдиної системи стандартизації документів

Щоб система документації була стрункою, слід, перш за все, чітко визначитися із системою класифікації документації та її кодування.

Застосування системи класифікації та кодування інформації дає можливість упорядкувати документи, що значно полегшить процес каталогізації документації як окремих підприємств, так і документів загального призначення.

ІІ. Автоматизація створення каталогів документів

1. Переваги автоматизації документообігу

Стандартизація та каталогізація документів сприяє економії часу й коштів підприємства. Користь від впровадження автоматизованих систем діловодства помітна не одразу, але не можна недооцінювати економічний ефект від покращення організації підприємства. За даними Ernst & Young та Nortan Nolan Institute у підприємств, які запровадили систему електронного документообігу, покращилися показники: показник ефективності праці в офісі збільшується на 25-50%; витрати часу на обробку документу зменшується на 75%; витрати на оплату площі для зберігання документів зменшуються на 80%. Зрозуміло, що ці критерії розроблялися для західного ринку, і в Україні ці цифри можуть мати дещо інший характер. Зокрема, користь від зменшення площі зберігання документів може бути значно меншою, оскільки в нашій країні й на далі юридичну силу мають лише паперові документи або їхні мікрокопії. У той же час зменшення часу на обробку документів і чітке дотримання регламенту обробки документа у багатьох сферах є критичними показниками, які можуть принести більший економічний ефект від запровадження автоматизованої системи діловодства.

2. База даних як одиниця автоматизації системи документообігу

Автоматизація документообігу вимагає стрункої системи каталогізації документів. Каталоги створюються за різними ознаками класифікації документів і повинні бути зручними й простими у використанні, що полегшить пошук потрібних документів у разі потреби. Основою каталогів є бази даних документації.

Під поняттям „база даних” розуміють упорядкований набір даних, у технічному розумінні виключно й система керування базою даних.

Головним завданням бази даних є гарантоване збереження значних обсягів інформації (так звані записи даних) та надання доступу до неї користувачеві або ж прикладній програмі. Таким чином база даних складається з двох частин — інформації, що запам’ятовується, та системи управління нею. З метою забезпечення ефективності доступу записи даних організовують як множину фактів (елемент даних).

3. Програми із систематизованого обліку документів

На сьогоднішній день на українському ринку є кілька програм із системи обліку документів.

Однією з таких програм є система обліку документів „Канцелярія”, що призначена для автоматизації документообігу на підприємствах різного профілю й масштабу. На відміну від програмного продукту „Система учета документов «Канцелярия»” інтерфейс та усі текстові повідомлення виконані українською мовою.

ІІІ. Можливості використання інтернет-технологій для автоматизації каталогізації документів

Каталогізація документів проводиться з метою систематизування документів державного масштабу чи документів певної організації, підприємства. Каталоги – ключ до довідково-інформаційного забезпечення

діяльності підприємств, організацій, державних установ, зокрема їх можна вважати своєрідним довідниками – збірниками нормативно-правових актів, шаблонів документів тощо.

Висновки. Отже, збільшення об’ємів документообігу на сучасному етапі розвитку суспільства змушує запроваджувати роботу з новими джерелами інформації, удосконалювати форми документообігу, розробляти процеси автоматизації. Створення автоматизованих каталогів документів залишається однією з пріоритетних задач.

Література

1. С.В. Поперешняк Актуальна проблема електронного документообігу– нестача дискового простору / С.В. Поперешняк, О.І. Недбайло // Вісник соціально-економічних досліджень. – 2013. – С. 147-152
2. Поперешняк С.В Сучасні проблеми електронного документообігу на прикладі системи «ДІЛО» /Недбайло О.І. Поперешняк С.В // Економіка підприємства: сучасні проблеми теорії та практики. – 2012. – С. 97-98
3. С.В. Поперешняк Інформаційні системи холдингових організацій та система управління взаємовідносинами з клієнтами // ДонНТУ. – 2010. – URI : http://ea. donntu. edu.ua /handle/123456789/18533

Вєчерковська А.С.
асистент кафедри Програмних систем і технологій
Київський національний університет імені Тараса Шевченка
Клімко В.В.
студент кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

СИСТЕМИ АВТОМАТИЗАЦІЇ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

Стратегія розвитку сучасного виробництва передбачає істотне підвищення рівня автоматизації, перш за все, технологічних процесів(ТП), при реалізації яких вихідна сировина, матеріали перетворюються в закінчений продукт. Однак, сьогодні, технологічні процеси є дуже складними, та іноді небезпечними особливо при роботі з хімічними матеріалами, можливості людини обмежені. При роботі з полімерними матеріалами давно шукають переходи до безперервного потоку, який значно легше піддається автоматизації.

Автоматизація- це застосування у виробництві технічних засобів, методів і систем управління, які звільняють людину від безпосередньої участі у виробництві. Метою автоматизації полягає в підвищенні продуктивності і ефективності праці, поліпшення якості продукції та умов трудової діяльності людини.[1]

Перебіг ТП і технічний стан обладнання в кожен момент часу характеризується різними фізичними величинами: зусиллям, тиском, температурою, переміщенням, швидкістю, прискоренням, витратою рідини і газу, електричною напругою, силою струму і т. д. Під час ТП і роботи обладнання безперервно змінюються. Рівень і якість автоматичного контролю, регулювання та сигналізації визначає точність і надійність вимірювальних приладів. Для здійснення контролю оператор, повинен отримувати відомості про значення технологічних параметрів і про їх зміну в зручному для нього вигляді, найкраще перебуваючи у віддалені від технологічного обладнання у вигляді результату виконання комп`ютерної програми, або мобільного застосунку, тобто необхідне узагальнення, аналіз і прогноз.

Отримана в процесі контролю інформація використовується для впливу на технологічне обладнання у вигляді команди з метою забезпечення протікання ТП в повній відповідності з запланованим його ходом, тобто для управління технологічним процесом. Ця послідовність виконання дій, що веде до досягнення певної мети, називається алгоритмом управління, яку необхідно передбачити при плануванні і проектуванні автоматизованої системи, та алгоритму її роботи.

Таким чином, контроль ТП включає в себе алгоритми збору, обробки та аналізу інформації, видачу оператору повідомлень про хід ТП і роботи обладнання. Для цього найкраще використовувати мобільні застосування, або комп'ютерні програми, що підняло б рівень автоматизації технологічних процесів на новий, більш високий рівень, і забезпечило б безпеку роботи на підприємствах хімічної промисловості.

Література

1. Михеев, В. А. Автоматизация процессов ОМД [Электронный ресурс]

Берестов Д.С.
к.т.н., заступник начальника науково-дослідного управління центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського
Зотова І.Г.
провідний науковий співробітник центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського
м. Київ, Україна

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТЕХНОЛОГІЇ INTERNET OF EVERYTHING (IoE)

Основна цінність технології IoE дані, що збираються з усіх інтелектуальних пристроїв та направляються для обробки за допомогою технологій Big Data, що дозволяє прив'язати всі об'єкти до конкретних користувачів, і дає можливість добитися максимальної персоналізації рішень і оперативного усунення проблем користувачів. Сучасні технології обробки даних не завжди гарантують контроль з боку користувачів, частково переходячи у владу операторів сервісів.

Саме тому важливою вимогою до систем IoE є збереження приватності користувачів.

Захист технології IoE у цілому повинен опиратися на надійну аутентифікацію, гнучкі та контрольовані користувачем привілею доступу до обчислювальних ресурсів, шифрування даних.

Механізм керування привілеями додатків є в мобільних операційних системах, таких як Android, IOS і Windows Phone, однак він не стандартизований, залежить від операційної системи, надаючи користувачам зовсім різні можливості, що приводить до помилок і росту ризику атак. Необхідно провести процес стандартизації механізмів керування різними пристроями і привілеями доступу до них по моделі, яка зараз існує у виробників мобільних операційних систем.

Підключені до Інтернету пристрої, встановлені на різних об'єктах, таких як автомобілі, побутова техніка та іграшки, можуть бути використані для незаконного спостереження, дозволяючи злочинцям не тільки пасивно стежити за їх жертвами та активно вторгатися в їх особисте життя, одержувати набагато більше інформації про особу. Причина в тому, що багато з підключених до Інтернету пристроїв, встановлені в об'єктах, які можуть бути дистанційно керованими.

Вищезгадані загрози конфіденційності демонструють необхідність врегулювання технології IoE. Зменшуючи ризики пов'язані з приватністю, ми дозволимо технології IoE розбудовуватися в напрямку, що дозволить поліпшити різні аспекти життя людей.

Федорієнко В.А.
старший науковий співробітник центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського
м. Київ, Україна

ДЕЯКІ АСПЕКТИ ТЕХНОЛОГІЇ IoE ЩОДО ФІКСАЦІЇ ПОРУШЕНЬ МІНСЬКИХ ДОМОВЛЕНОСТЕЙ У КОНФЛІКТІ НА СХОДІ УКРАЇНИ

У рамках збройного конфлікту на сході України все частіше виникає потреба використовувати системи із рівнями мобільних пристроїв (датчиків збору даних), обробки, аналізу та публікації даних. Практична реалізація подібної схеми була апробована на робочому макеті інформаційно-аналітичної системи фіксації обстрілів (ІАСФ) [1], яка у певній мірі здатна підвищити рівень автоматизації за рахунок реалізації механізму швидкої візуалізації та аналізу обстановки на рівні баз даних для забезпечення інформаційних потреб Української сторони Спільного центру з контролю та координації питань припинення вогню та стабілізації лінії розмежування сторін (СЦКК), що взаємодіє із Спеціальною моніторинговою місією ОБСЄ [2].

Сьогодні, світова спільнота, разом із залученими міжнародними організаціями під егідою ООН, прагне отримувати правдиву картину зі Сходу України, наприклад, інформацію щодо порушень режиму тиші. При цьому важливо відповідати вимогам щодо точності та оперативності. Тобто, постійно бути у готовності щодо висвітлення порушень Мінських домовленостей та шкоди завданої цивільним особам.

Мережева складова інформаційного середовища ІАСФ, для передачі даних про факт обстрілу з боку незаконних збройних формувань (НЗФ), у СЦКК розглядалася, як відкрита інформація, що дозволяє використовувати мережу Інтернет, і, відповідно, застосовувати концепцію Internet of Everything (IoE). Поняття "IoE" визначається, як технологія, що "об'єднує людей, процес, дані та речі, щоб утворювати мережеві зв'язки більш релевантними та цінними, перетворюючи інформацію у дії, що створюють нові можливості, багатший досвід та безпрецедентні економічні можливості для бізнесу, окремих осіб та країн" (Cisco, 2013) [3]. При цьому, IoE спирається на чотири концептуальні “стовпи” (основи), а саме: 1. Люди (спілкування людей здійснюється більш релевантними та ціннісними способами), 2. Дані (перетворення даних в аналітику для прийняття кращих рішень), 3. Процес (надання потрібної інформації визначеній людині (або машині) в потрібний час), 4. Речі (фізичні пристрої та об'єкти, підключені до Інтернету та один до одного для розумного прийняття рішень; часто називається Internet of Things або IoT).

Для створення макету ІАСФ була вирішена низка наукових та прикладних завдань, серед них: здійснено формалізацію процесів діяльності СЦКК в анотаціях BPMN 2.0; проведені дослідження проблемних питань автоматизації процесів збору, реєстрації, зберігання, аналізу і відображення на електронній карті фактів порушення режимів припинення вогню, що цілком відповідає концептуальним основам IoE.

Закцентуємо увагу на п’ятьох етапах IoE, які частково співставленні із функціями ІАСФ, що відображують трансформацію даних в цінну інформацію: 1. Підключення пристроїв, 2. Збір даних, 3. Доступ до даних, 4. Комплексний аналіз, 5. Унікальна цінність. Типами комунікації є: людина-машина (Human-to-Machine, H2M), людина-людина (Human-to-Human, H2H); машина-людина (Machine-to-Human, M2H), машина-машина (Machine-to-Machine, M2M).

На першому етапі – здійснюється підключення пристрою до мережі інтернет (вхід у хмару на портал організації СЦКК, ввівши логін і пароль, завантаження встановленого фрагменту карти у залежності від присвоєної ролі) активуються прийомні датчики GPS тощо (edge computing) – M2M, H2M.

На другому етапі – здійснюється збір та накопичення даних на мобільних пристроях за рахунок вводу та приєднання медіа вмісту – M2H.

На третьому етапі – здійснюється авторизований доступ до хмари (cloud) організації та синхронізація даних (із пристроїв), виконуються вимоги стандартів обміну даними та OGC (Open Geospatial Consortium) – M2M.

На четвертому етапі – здійснюється статистичний та геопросторовий аналіз даних, може здійснюватися на рівні хмари, ГІС-серверу (fog computing), серверу додатку BI (Business Intelligence), чи робочої станції (Desktop) із повторною публікацією в хмарі – M2M, M2H, H2H.

На п’ятому етапі – реалізований справжній потенціал підключеної спільноти до порталу візуалізації наслідків обстрілів та завданої шкоди цивільним об’єктам для їх подальшого моніторингу та аналізу –M2H.

Незважаючи, що переваги спільного аналізу даних можуть забезпечити перевагу швидкого висвітлення інформації про обстріли, важливим завданням є вирішення проблемних питань безпеки. З точки зору кібернетичної загрози, під основним ризиком розуміють загрозу даним або фізичній безпеці системи, що становить 42 % від загального числа недоліків IoE зазначених у [4].

Література

1. Тимошенко Р. І. Аспекти практичної реалізації макету інформаційно-аналітичної системи фіксації обстрілів для Української сторони СЦКК / Р. І. Тимошенко, Федорієнко В. А., О. В. Головченко. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2017. – №3. – С. 84–88.

2. Рамочное решение Трёхсторонней контактной группы о разведении сил и средств [Електронний ресурс] // OSCE CMM of Ukraine. – 2016. – Режим доступу до ресурсу: http://www.osce.org/ru/cio/266271?download=true.

3. Banafa A. The Internet of Everything (IoE) [Електронний ресурс] / Ahmed Banafa // Open Mind. – 2016. – Режим доступу до ресурсу: https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe/.

4. GREENOUGH J. The 'Internet of Things' will create a lot of security vulnerabilities -- here are ways companies can start tackling these issues [Електронний ресурс] / JOHN GREENOUGH // Business Insider. – 2015. – Режим доступу до ресурсу: https://www.businessinsider.com.au/ftc-top-recommendations-for-protecting-home-iot-2015-3.

Кондратенко Ю.В.
старший науковий співробітник центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського
м. Київ, Україна

АНАЛІЗ СТАНУ ЗАХИЩЕНОСТІ INTERNET OF THINGS

Інтернет речей (IoT) знаходиться тільки на початковій стадії свого розвитку, але вже розвивається з достатньою швидкістю, і всі нововведення додають серйозні проблеми, пов'язані з інформаційною безпекою.

З поширенням концепції «Інтернет речей» є нагальною потребою забезпечити унікальність ідентифікаторів об'єктів, що, в свою чергу, вимагає стандартизації.

Для об'єктів, безпосередньо підключених до мережі Інтернет, традиційний ідентифікатор - MAC-адреса мережевого адаптера, що дозволяє ідентифікувати пристрій на канальному рівні, при цьому діапазон доступних адрес практично вичерпується, а використання ідентифікатора канального рівня не дуже зручне для додатків. Ширші можливості по ідентифікації для таких пристроїв дає протокол IPv6, що забезпечує унікальними адресами для мережевого обладнання.

Всі речі (складові «Інтернет речей») для підключення до Інтернет мають операційну систему (як правило, досить урізану), реалізацію мережевого стека (для підключення до мережі) і прикладну частину, яка встановлюється на ОС.

Відповідно, по мережі з великою ймовірністю з Інтернет буде доступне управління такими компонентами як операційна система (по засобом SSH або telnet) і додатки (через web-interface або власні розробки). Взлом призведе до компрометації даних, повного контролю над пристроєм, перехоплення управління і використання як майданчика для хакерських атак.

Для забезпечення захисту пристроїв необхідно проводити заходи щодо виділення окремого сегмента мережі, контролю цілісності системних файлів, резервного копіювання, моделювання загроз IoT і розробці варіантів захисту на всіх рівнях, контролю зміни конфігурації і вразливостей, жорстке управління оновленнями та парольними політиками.

Отже, якість налаштування безпеки кожного конкретного компонента має ключове значення для безпеки всієї інфраструктури IoT.

Література

1. Internet Of Things (англ.). Gartner IT glossary. Gartner (5 May 2012).
2. Dave Evans. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything (англ.). Cisco White Paper. Cisco Systems (2011).
3. Neil Gershenfeld, Raffi Krikorian, Danny Cohen. The Internet of Things (англ.). Scientific American, Oct, 2004.
4. Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli. Fog Computing and Its Role in the Internet of Things. SIGCOMM’2012. ACM (2012).

Кузніченко С.Д.
к.геогр.н., доц.
Одеський державний екологічний університет
Бучинська І.В.
аспірант
Одеський державний екологічний університет
м. Одеса, Україна

ПРОЕКТУВАННЯ ІНТЕГРОВАНОЇ ГЕОІНФОРМАЦІЙНОЇ СИСТЕМИ РЕГІОНАЛЬНОГО МОНІТОРИНГУ ПОВЕНЕЙ НА ОСНОВІ IoT

Останнім часом геоінформаційні системи знаходять все більш широке застосування при моделюванні різних природних процесів і явищ: паводків, посух, снігопадів, лісових пожеж тощо [1]. Одним з найнебезпечніших стихійних лих є паводки, негативні наслідки від прояву яких відчуваються в середньому на 27% території України. Надійний моніторинг і прогнозування паводків дуже важливі для підтримки прийняття рішень для попередження, запобігання та пом'якшення наслідків лиха відповідними адміністративними органами.

У зв’язку з цим досить актуальним є створення ГІС-орієнтованої інтегрованої інформаційної системи реального часу для регіонального моніторингу та прогнозування повеней. Подібна система як правило інтегрує бездротову сенсорну мережу для збору метеорологічних та гідрологічних даних в інтерактивному режимі, тобто будується за технологію Інтернет речей (Internet of Things, IoT) [2].

Можливості по створенню інформаційних систем подібного класу зростають з кожним роком і обумовлюються з одного боку підвищенням просторової і часової здатності вимірювального обладнання, точності та детальності значень, що реєструються, з іншого боку вдосконаленням сенсорів; технології радіочастотного розпізнавання (Radio Frequency Identification, RFID), призначеної для ідентифікації керуючих елементів за допомогою мікросхем-міток; процесорів, що мають низьку вартість і можуть проводити мобільні обчислення з використанням Інтернету (аналіз великих даних, що поступають від сенсорів); бездротових сенсорних мереж (WSN), які дозволяють створювати розподілені, самоорганізаційні мережі датчиків і пристроїв, що самостійно зв'язуються радіоканалом; енергоефективних технологій передачі даних (наприклад, Bluetooth Low Energy (BLE), Near Field Communication (NFC); телекомунікаційних технологій.

Розвиток технологій IoT зумовив зростання обсягів даних, які стає складно обробляти за допомогою інструментальних засобів керування даними СКБД і традиційних застосувань обробки даних. Тому важливим є передбачити збереження Big Data у сховищах даних чи за допомогою хмарних технологій.

Загальна структура системи регіонального моніторингу повеней на основі IoT наведена на рис.1. Для збору даних про навколишнє середовище в режимі реального часу використовується бездротова сенсорна мережа, яка складається з окремих сенсорів з автономними джерелами живлення. Сенсорний вузол є

вузлом базової мережі, який відповідає за збір даних. Кожний датчик автоматично шукає приймач даних за відповідною мережевою адресою. Кожна мережа датчиків має шлюз для підключення сенсорної мережі до зовнішньої мережі (рис.2).

Рисунок 1–Загальна структура інтегрованої інформаційної системи на основі IoT

Через шлюз інформація може бути передана до центру моніторингу за допомогою мережі Інтернет (Ethernet, Wi-Fi, 3G/GPRS). Для збору даних у режимі реального часу можуть бути використанні засоби дистанційного зондування [3] (тобто супутники, повітряні кульки, літаки та радар), мобільні пристрої (тобто GPS, 2G, 3G, 4G та LTE), IEEE 802.X (тобто WiFi, Bluetooth і ZigBee), RFID та інші датчики.

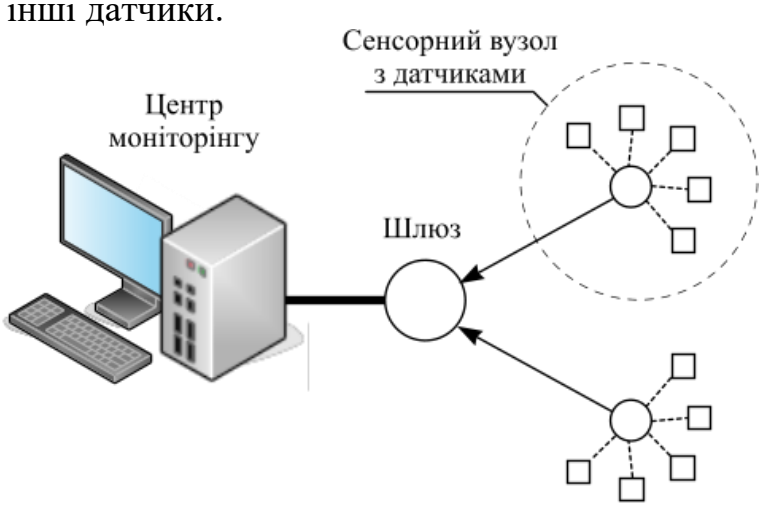


Рисунок 2–Структура бездротової сенсорної мережі

Дані моніторингу поступають у сховище геоданих і можуть бути використані у просторовому моделюванні і ГІС-аналізі з використанням спеціальних бібліотек ГІС платформи (ArcGIS, QGIS, MapInfo) для побудови карти ризику повеней. Кожний критерій, який враховується при побудові карти представляється у вигляді векторного чи растрового шару. Карти просторового розподілу опадів та вологості грантів можуть бути отримані шляхом інтерполяції за опорними точкам, які містять значення, отримані від бездротової сенсорної мережі.

Карта ризику повеней може бути отримана шляхом використання мультикритеріальних методів аналізу рішень MCDA в ГІС [4], наприклад, булевого накладання (Boolean Overlays), зваженої лінійної комбінації (WLC),

аналізу ієрархій (AHP) і упорядкованого середнього зваженого (OWA). Отримана карта може бути використана для підтримки прийняття рішень щодо заходів для попередження, запобігання та пом'якшення наслідків лиха відповідними адміністративними органами.

Література

1. Tomaszewski B. (2014) Geographic information systems (GIS) for disaster management. CRC Press, 297.

2. Dr. V. Bhuvaneswari, Dr. R Porkodi, “The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview”, International Conference on Intelligent Computing Applications, 2014, pp. 324-329

3. Перелигін, Б. В. Методи і засоби обробки моніторингової інформації [Текст] / Б.В.Перелигін, С.Д. Кузниченко. – Одеса: ЕКОЛОГІЯ, 2010. – 224 с.

4. Malczewski J., Rinner C. (2015) Multicriteria Decision Analysis in Geographic Information Science. Springer Science+Business Media New York, 331

Мамука К.В.
магістр
Одеський державний екологічний університет
Кузніченко С.Д.
к.геогр.н., доц
Одеський державний екологічний університет
м. Одеса, Україна

МЕТОДИ ЕВОЛЮЦІЇ НЕЙРОННИХ МЕРЕЖ В ПРОЦЕСІ СВОГО НАВЧАННЯ ТА ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В ІНТЕРНЕТІ РЕЧЕЙ

Інтернет речей – це загальний термін, що характеризує інтеграцію Інтернету в фізичний світ, при його широкому поширенні і впровадженні в фізичні об'єкти з метою розширення їх можливостей. Концепція Інтернету речей має на увазі світ, в якому фізичні та цифрові об'єкти будуть тісно пов'язані між собою, даючи тим самим початок новому поколінню послуг і додатків з використанням відповідних систем.

Інтернет речей здатний влаштувати наше життя набагато розумнішим. Ці інноваційні технології забезпечують зручність в повсякденній діяльності, енергоефективність, безпеку і комфорт. Також додавання розумних технологій в домашню сферу може підвищити якість життя хворих і літніх людей.

У 2016-2017 роках світу продемонстрували безліч розробок в області нейронних мереж – свої алгоритми демонстрували Google, Microsoft, стартапи та інші. Нейронні мережі – один з напрямків в розробці систем штучного інтелекту. Ідея полягає в тому, щоб максимально близько змоделювати роботу людської нервової системи – а саме, її здатності до навчання і виправлення помилок. У цьому полягає головна особливість будь-якої нейронної мережі – вона здатна самостійно навчатися і діяти на підставі попереднього досвіду, з кожним разом роблячи все менше помилок.

Нейронні мережі здатні вирішувати такі ж завдання, як і інші алгоритми машинного навчання, різниця полягає лише в підході до навчання. Тому всі завдання, які можуть вирішувати нейронні мережі, так чи інакше пов'язані з навчанням. Серед основних областей застосування нейронних мереж: прогнозування, прийняття рішень, розпізнавання образів, оптимізація і аналіз даних.

Сьогодні нейромережі використовуються повсюдно, вони лежать в основі більшості сучасних систем розпізнавання і синтезу мови, а також розпізнавання і обробки зображень. Вони застосовуються в деяких системах навігації, будь то промислові роботи або безпілотні автомобілі. Алгоритми на основі нейромереж захищають інформаційні системи від атак зловмисників і допомагають виявляти незаконний контент в мережі. А в найближчій час нейронні мережі будуть використовуватися ще ширше.

На жаль, штучні нейронні мережі призначені для вирішення будь-якого спеціалізованого завдання. В основному це завдання класифікації (розпізнавання образів). Якщо розглядати алгоритми, які дозволяють навчити нейронну мережу, що складається з відносно невеликого числа нейронів (наприклад кількох сотень), то кожен з алгоритмів не гарантує оптимального результату і вимагає внесення змін під кожну конкретну задачу. У такій навченої нейронної мережі вкрай важко аналізувати

зміст ваг того чи іншого нейрона і значення його зв'язків. Можна аналізувати тільки всю мережу цілком – як інструмент, створений для вирішення певної задачі.

Вибір топології і настройка ваг зв'язків штучної нейронної мережі є одними з найважливіших етапів при використанні нейромережевих технологій для вирішення практичних завдань. Від цих етапів безпосередньо залежить якість отриманої нейронної мережі. Побудова штучної нейронної мережі за традиційною методикою виконується, фактично, методом проб і помилок. Розробник ставить кількість шарів, нейронів, а також структуру зв'язків між ними (наявність / відсутність зворотних зв'язків), а потім мережа навчається за допомогою будь-якого методу. Після тестується на тестовій вибірці. Якщо отримані результати роботи задовольняють заданим критеріям, то завдання побудови нейронної мережі вважається виконаним успішно; в іншому випадку – процес повторюється з іншими значеннями вихідних параметрів.

Але ж Природа побудувала біологічні нейронні мережі без «розуміння» їх кінцевої мети. Просто в результаті мутацій з'являлися нейрони з новими властивостями, збільшувалася їх кількість, виникали нові зв'язки, і це призводило до появи нових корисних якостей організму. Так як Природа наочно продемонструвала вирішуваність завдання еволюції нейронної мережі на прикладі еволюції нервової системи з подальшим утворенням і розвитком головного мозку, бурхливий розвиток теорії і практики використання генетичних алгоритмів, дозволяє шукати способи застосувати їх до задачі оптимальної структури штучної нейронної мережі. Генетичні алгоритми – адаптивні методи пошуку, які часто використовуються для вирішення завдань оптимізації. Вони засновані на генетичних процесах біологічних організмів: біологічні популяції розвиваються протягом декількох поколінь, підкоряючись законам природного відбору і за принципом "виживає найбільш пристосований", відкритого Чарльзом Дарвіном. Наслідуючи цьому процесу генетичні алгоритми здатні "розвивати" вирішення реальних завдань.

Центральною точкою будь-якого методу еволюційної побудови нейронних мереж є вибір генетичного уявлення. В даний час виділяють два великі класи способів кодування: пряме кодування і непряме кодування.

Пряме кодування оперує хромосомами, що представляють деякий лінійне уявлення нейронної мережі, в якому в явному вигляді вказані всі нейрони, ваги і зв'язку. Таким чином, завжди можна побудувати взаємно-однозначна відповідність між структурними елементами: нейронами, зв'язками, вагами та ін., Тобто фенотипом, і відповідними ділянками хромосоми, тобто генотипом. Цей спосіб представлення нейронної мережі є найбільш простим і інтуїтивним, а також дозволяє застосовувати до отриманих хромосомами вже наявний апарат генетичного пошуку. З найбільш очевидних мінусів такої схеми кодування можна відзначити «розпухання» генотипу при збільшенні кількості нейронів і зв'язків, і, як наслідок, низьку ефективність за рахунок значного збільшення простору пошуку. Варто відзначити, що є методики метою яких є купірування вищеописаних недоліків, наприклад, NEAT.

Непряме кодування демонструє більш «біологічно» принцип – в генотипі кодується не саме фенотип, а правила його побудови. При декодуванні генотипу ці правила застосовуються в певній послідовності (найчастіше, рекурсивно і,

найчастіше, застосовність правил залежить від поточного контексту), в результаті чого і будується нейронна мережа.

При використанні непрямих методів кодування генетичне уявлення (а, відповідно, і простір пошуку для генетичних алгоритмів) виходить більш компактним, а сам генотип дозволяє кодувати модульні структури, що дає в певних умовах переваги в адаптивності отриманих результатів. Значним недоліком є складність простежити, які зміни в генотипі привели до заданих змін у фенотипі, а також безліч труднощів з підбором генетичних операторів, збіжністю і продуктивністю. Але сучасні підходи, дозволяють позбутися від цих недоліків.

Застосування непрямих методів кодування більш перспективно, адже відповідно до сучасної нейрології, неможливо прямо і незалежно описати закодованої в хромосомах генетичною інформацією всю нервову систему. Такий висновок випливає, наприклад, з факту, що генотип людини складається з набагато меншої кількості генів, ніж число нейронів в його мозку.

Використання генетичних алгоритмів при побудові і навчанні нейронних мереж, можливість змін нейронної мережі в процесі роботи – дозволять наблизиться до побудови універсальної нейронної мережі, яка здатна буде вирішувати всілякі завдання і не вимагати коригування під кожну спеціалізовану задачу. Це наблизить людство до створення штучного інтелекту, схожого людині, адже якщо Природа створила нервову систему, то ми можемо створити штучний інтелект ґрунтуючись на біологічних принципах нервової системи і головного мозку.

Дослідники Інтернету речей стверджують, що всі об'єкти в майбутньому матимуть унікальні можливості ідентифікації, що посприяє об'єднанню їх в одну мережу і формування Інтернету речей. Глобальна комунікація, як наслідок, перестане бути просто зв'язком між людьми і стане зв'язком між людьми і речами, що кардинально змінить життя. Об’єднання всіх об’єктів в глобальну мережу Інтернету речей – дає неймовірні можливості для допомоги людям, наприклад, система регулювання автомобільним рухом мегаполісу, яка буде керувати світлофорами та пропонувати машинам обирати інший маршрут – о заторах можна буде забути. Це лиш один з прикладів, яких можна привести безліч. З такими задачами зможе справитись тільки нейронна мережа, а враховуючи кількість завдань, які доведеться вирішувати необхідний швидкий, гнучкий і універсальний алгоритм нейронної мережі.

Інтеграція нейронних мереж до Інтернету речей надасть неймовірні можливості для людства.

Література

1. Darrel Whitley. A Genetic Algorithm Tutorial, 1993.
2. Stanley K.O., Miikkulainen R. Evolving Neural Networks through Augmenting Topologies, 2002.
3. Цой Ю.Р., Спицын В.Г. Эволюционный подход к настройке и обучению искусственных нейронных сетей, 2006.
4. Risto Miikkulainen, Kenneth O. Stanley. Evolving Neural Networks, 2009.
5. Kevin Ashton. That ‘Internet of Things’ Thing. In the real world, things matter more than ideas, 2009.

Михайлова А.В., Тесленко О.М.
Український науково-дослідний інститут цивільного захисту
Чумаченко С.М.
Державна установа «Інститут геохімії навколишнього середовища» НАН України
м. Київ, Україна

МЕТОДИ ЕКСПЕРТНОЇ ОЦІНКИ, ЯК ІНСТРУМЕНТ ОЦІНЮВАННЯ ХАРАКТЕРИСТИК ІНТЕГРОВАНИХ СИСТЕМ МОНІТОРИНГУ ТА ОПОВІЩЕННЯ

Статистика виникнення надзвичайних ситуацій (далі – НС) різного походження в нашій країні [1] свідчить про високий рівень небезпеки та ризику, тому система моніторингу та оповіщення про загрозу або виникнення НС, котра належить до компетенції ДСНС України [2] повинна працювати налагоджено, безперебійно, надійно, бути науково обґрунтованою й практично верифікованою.

Зважаючи унікальність кожної НС та у зв'язку з неможливістю математичної формалізації процесу рішення, постає необхідність звернення до рекомендацій експертів. Таким чином, для здійснення обґрунтування технічних характеристик до системи моніторингу та оповіщення найефективнішим є застосування експертно-аналітичних підходів.

Всі методи експертних оцінок поділяються на індивідуальні та колективні [3], кожен з яких має свої переваги та недоліки. Проте, вигідно вирізняється від решти методів метод аналізу ієрархій (далі - MAI) у зв'язку з простотою обчислень і надійними програмними засобами їх реалізації [4]. В даній роботі цей метод застосовано для оцінювання характеристик інтегрованих систем моніторингу та оповіщення про загрозу або виникнення НС. Детальний опис та роз'яснення його використання, тлумачення результатів, отриманих в результаті його застосування, тощо описано в [5].

З метою визначення пріоритетних характеристик інтегрованих систем моніторингу та оповіщення про загрозу або виникнення НС використано програмний додаток, що реалізує MAI й атрибути інтегрованої системи моніторингу та оповіщення про загрозу і виникнення НС, наведені в [6]. Будується трирівнева ієрархія та здійснюється попарне порівняння кожної з підхарактеристик.

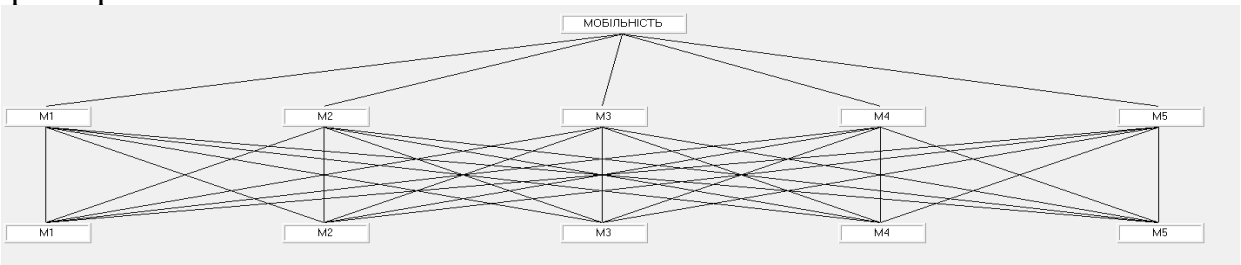


Рисунок 1. Приклад ієрархії з оцінювання пріоритетних під характеристик одного з атрибутів інтегрованої системи моніторингу та оповіщення про загрозу або виникнення НС

В результаті проведеної роботи фахівцями експертної групи отримано пріоритети в кожній групі підхарактеристик, а саме: точність та відповідність нормам функціональності; відповідність нормам надійності; змінність; замінність і т.ін.

Таким чином, отримані результати дають можливість їх врахування під час розробки інтегральної системи моніторингу та оповіщення про загрозу або виникнення НС. Доведено можливість ефективного застосування методів експертної оцінки, зокрема методу аналізу ієрархій, для оцінювання характеристик вищезазначених систем, що дозволить науково обґрунтувати технічні вимоги для їх розробки.

Література

1. Аналітичний огляд стану техногенної та природної безпеки в Україні за 2016 рік [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://undicz.dsns.gov.ua/ua/Analitichniy-oglyad-stanu-tehnogennoyi-ta-prirodnoyi-bezpeki-v-Ukrayini.html.

2. Кодекс цивільного захисту України: чинне законодавство із змінами та доповненнями [Офіційний текст] – К.: Видавець – ФОП Паливода А.В. 2016. – 131 с.

3. Методы экспертных оценок [Електронний ресурс] – Режим доступу до ресурсу: http://uchebnik.online/sotsialno-ekonomicheskih-prognozirovanie/metodyi-ekspertnyih-otsenok-32524.html.

4. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А. Б. Качинський. – Київ, 2004. – 472 с.

5. Саати Т., Кернс К. Аналитическое планирование. Организация систем: Пер. с англ.- М.: Радио и связь, 1991 .- 224 с.

6. Михайлова А. В. Модель оцінки якості інтегрованих систем моніторингу та оповіщення про загрозу або виникнення надзвичайної ситуації / А. В. Михайлова, С. М. Чумаченко. // iScience. Актуальные научные исследования в современном мире. Сборник научных трудов. – 2017. – №8. – С. 76–80.

Пашинська Н.М.
к.геогр.н., старший науковий співробітник кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ГІС ДЛЯ ОБРОБКИ ДАНИХ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

Величезна кількість даних щоденно передається з різних сенсорів і пристроїв: GPS-приймачів на транспорті, різних об'єктах і у людей, сенсорного моніторингу навколишнього середовища, відеопотоків в реальному часі, з соціальних мереж і багатьох інших, пов'язаних між собою через Інтернет. Більшість з цих потоків даних в веб має просторову прив'язку, тобто може бути зібрано, організовано, проаналізовано та візуалізовано за допомогою ГІС.

Одним із сучасних напрямів розвитку ГІС є ГІС в реальному часі, які можна охарактеризувати як безперервний потік подій, що надходить з датчиків інтернету речей або з джерел даних. Кожна подія представляє останній виміряний стан, включаючи місце розташування, температуру, концентрацію, тиск, електрична напруга, рівень води, висоту, швидкість, відстань і інформацію про направлення, що надходить з сенсора. Ці дані можуть бути візуалізовані за допомогою карти, що є основною для перегляду, моніторингу та реагування на надходження даних в реальному часі.

В основі концепції Internet of Everything (IoT) є «речі», які передають свої дані в різні мережі та Інтернет. Основна ідея полягає в тому, що з часом все більше оточуючих нас речей і об'єктів будуть підключені до Інтернету і об'єднані в єдину мережу для більш точного вимірювання і розуміння процесів. Це нове, величезне і різноманітне джерело даних, які можна використовувати в системах, що здійснюють моніторинг, аналізують дані і навіть автоматично віддають команди іншим системам і додаткам [1]. В останні роки наукова спільнота, державні організації та комерційні компанії, почало застосовувати концепції IoT для створення різних систем і продуктів, від систем управління домашніми електроприладами до систем комунальних мереж, які керують розподілом і споживанням електроенергії.

Концепції IoT можуть мають велику кількість практичних застосувань в середовищі ГІС для динамічних геопросторових вимірювань як в природному середовищі (наприклад, вологості ґрунту, річкового стоку, розвитку рослин), так і в антропогенному (в будівництві, енергетиці, для вимірювання рівня шуму і транспортних потоків). IoT займає центральне місце в концепції «розумних» міст, і в поєднанні з ГІС може підтримувати різні додатки, моніторинг і створення звітів про стан різних міських та відомчих систем.

ГІС забезпечує практичний спосіб організації сенсорних даних реального часу в «шари» даних, які можна відразу ж візуалізувати і аналізувати в ГІС. Відповідно для користувачів це новий, динамічний і цікавий масив інформації, який може збагатити їх існуючі програми і дозволити створити новий клас

додатків, які роблять організації «розумнішими». Одна з важливих переваг архітектури веб-ГІС полягає в можливості інтеграції даних реального часу, що надходять від різних датчиків. Веб-ГІС реального часу - це перспективна платформа для реалізації проектів «розумних» міст, комунальних мереж, урядів і організацій. Така інтеграція не тільки відкриває величезні перспективи для ГІС-фахівців і всієї геопросторової галузі, а й ставить нові завдання використання, відображення та аналізу таких даних реального часу спільно з даними з традиційних джерел [2].

Ознаками та властивостями ГІС як платформи є:

1. Архітектура веб-ГІС, яка: а) абстрагується і інтегрує всі типи геопросторових даних (шари і веб-карти); б) підтримує динамічні, «засновані на сервісах» просторовий аналіз і візуалізацію; в) містить готові програми з розвиненим функціоналом; г) має відкриту архітектуру і API для вбудовування/ розширення функціоналу.
2. Можливість інтегрувати і використовувати дані реального часу.
3. Можливість зберігати, організовувати і аналізувати дуже великі набори просторово-часових даних.
4. Інтерактивні додатки для пошуку та аналізу просторових даних.

В даний час системи ГІС реального часу доповнюють рішення інтернету речей, розширюючи можливості вбудовування безперервного аналізу в просторі-часі. Прикладом можуть служити автономні транспортні засоби, коли транспортний засіб звітує про місцезнаходження, а також стан на дорогах. Зібрані спостереження можуть використовуватися спільно для аналізу дорожніх умов і надання попереджень про труднощі руху і пошуку маршрутів об'їзду, якщо необхідно. Можливість поєднання інформації від безлічі типів датчиків і розташувань є критично важливим фактором для виконання складних операцій [3].

Ця інтеграція мереж різних датчиків об'єднується інтелектуальним чином в геопросторову оболонку для операцій оптимізації, і є одним з найбільш значущих моментів інтернету речей. Раніше різнорідні набори інформації тепер можуть бути об'єднані в реальному часі, для щоб виокремити всі можливі сторони проблеми і прийняти важливі рішення, таким чином поліпшуючи ефективність, оптимізуючи сервіси і зменшуючи витрати.

Література

1. Bari N., Mani G., Berkovich S. Internet of Things as a Methodological Concept // Computing for Geospatial Research and Application (COM.Geo), 2013
2. E., Scholten H. Application of geographical concepts and spatial technology to the Internet of Things // VU University, FEWEB-RE, 2013. - 50 p.
3. Geospatial modelling of data-based technologies are trending towards the IoT // https://www.geospatialworld.net/article/geospatial-modelling-data-based-technologies-trending-towards-internet-of-things/

Ткаченко М.В.
к.т.н.
Ляшуга М.В., Самойленко О.А., Табунов А.А.
студенти кафедри Програмних систем і технологій
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

НЕЙРОМЕРЕЖЕВІ АЛГОРИТМИ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ ЩОДО ВИКОРИСТАННЯ У INTERNET ТЕХНОЛОГІЯХ

Виконано огляд нейромережевих алгоритмів, що використовуються при розпізнаванні графічного контенту сайтів. Нейромережеві алгоритми - це методи, що базуються на застосуванні різних типів нейронних мереж (НМ). Основні напрямки застосування різних НМ для розпізнавання графічного контенту сайтів:

- застосування для отримання ключових характеристик або ознак заданого графічного контенту;
- класифікація графічного контенту або вже витягнутих з них характеристик (в першому випадку витяг ключових характеристик відбувається неявно всередині мережі);
- рішення оптимізаційних завдань.

Архітектура штучних НМ має деяку схожість з природними нейронними мережами. НМ, призначені для вирішення різних завдань, можуть істотно відрізнятися алгоритмами функціонування, але їх основні характеристики вказані нижче [1-3].

НМ складається з елементів, які називаються формальними нейронами. Кожен нейрон перетворює набір сигналів, що надходять до нього на вхід у вихідний сигнал. Саме зв'язки між нейронами, які кодуються вагами, грають ключову роль. Одна з переваг НМ (а також недолік при реалізації їх на послідовній архітектурі) це те, що всі елементи можуть функціонувати паралельно, тим самим істотно підвищуючи ефективність вирішення завдання, особливо в обробці зображень. Крім того, НМ дозволяють ефективно вирішувати багато завдань, вони надають потужні гнучкі і універсальні механізми навчання, що є їх головною перевагою перед іншими методами [4,5] (імовірнісні методи, лінійні роздільники, вирішальні дерева тощо). Навчання позбавляє від необхідності вибирати ключові ознаки, їх значимість і відносини між ознаками. Але тим не менше вибір вихідного представлення вхідних даних (вектор в n-вимірному просторі, частотні характеристики, вейвлет тощо), істотно впливає на якість рішення і є окремою темою. НМ мають гарну узагальнюючою здатністю (краще ніж у вирішальних дерев [5]), тобто можуть

успішно поширювати досвід, отриманий на кінцевому навчальному наборі, на всю множину образів.

Розглянуто архітектури та особливості багатошарових НМ, мереж високого порядку, НМ Хопфилда, нейронних мереж Кохонена, когнітронів, проведено аналіз переваг і недоліків розглянутих мереж при використанні їх щодо розпізнаванню графічного контенту сайтів.

Література

1. Головко В.А. Нейроинтеллект: Теория и применения. Книга 1. Организация и обучение нейронных сетей с прямыми и обратными связями – Брест:БПИ, 1999, - 260с.

2. Головко В.А. Нейроинтеллект: Теория и применения. Книга 2. Самоорганизация, отказоустойчивость и применение нейронных сетей – Брест:БПИ, 1999, - 228с.

3. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика, 1992 – 184с.

4. Petrou M. Learning in Pattern Recognition. Lecture Notes in Artificial Intelligence – Machine Learning and Data Mining in Pattern Recognition, 1999, pp. 1-12.

5. Jacobsen X., Zscherpel U. and Perner P. A Comparison between Neural Networks and Decision Trees. Lecture Notes in Artificial Intelligence – Machine Learning and Data Mining in Pattern Recognition, 1999, pp. 144-158.

Кулида В.О.
студент кафедры Телекоммуникационных систем и сетей
Государственный университет телекоммуникаций
г. Киев, Украина

СОЦИАЛЬНЫЕ СЕТИ КАК ОРУДИЕ В РУКАХ КИБЕРПРЕСТУПНИКОВ

Причиняющие ущерб действия в киберпространстве стали достаточно безопасной и выгодной преступной деятельностью.

Ботнет [1] – компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

Вредоносное ПО, способное совершать нападения и осуществлять взлом финансовых систем, имеет свою стоимость, как любой другой товар. «Пастух» (или управляющий ботнетом) использует вредоносные программы для заражения и получения контроля над другими компьютерами.

Социальные сети [2, ст 10] также становятся сценой для социального активизма. Например, в сети Facebook есть приложение под названием «Causes» (англ. «мотив, идея»), где могут собираться и вести деятельность заинтересованные стороны. В одном из опубликованных примеров некий вебсайт призывал «добровольцев» бороться за свою идею. Желающие «подключиться к борьбе» должны были всего лишь загрузить предоставляемую на сайте программу, и программа сделает все остальное. На самом деле пользователь соглашался подключить свой компьютер к ботнету.

Социальные сети дают людям со сходными интересами возможность набора рекрутов в добровольческие «армии кибервоинов». Этот процесс крайне прост: для этого нужно всего лишь выполнить письменные инструкции или загрузить некое вредоносное ПО.

Литература

1. Ботнет [Електронний ресурс]. – Режим доступу до ресурса: https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82
2. Бутримас В. Тревожная тенденция [Електронний ресурс] / Витаутас Бутримас – Режим доступу до ресурса: http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V2N2_ru.pdf

Кулида В.О.
студент кафедры Телекоммуникационных систем и сетей
Государственный университет телекоммуникаций
г. Киев, Украина

ПРОБЛЕМЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В УКРАИНЕ

В стране не проводится системная работа по подготовке организаций к кибератакам. Ответственные госорганы слишком много внимания уделяют техническим аспектам в ущерб организационным. Для мониторинга и блокирования кибератак внедряются какие-то технические решения, осваиваются какие-то гранты. Но, к сожалению, этого недостаточно. Не делается то [1], что нужно делать в первую очередь:

1. Не распространяются индикаторы атак и образцы зловредного кода, чтобы другие организации могли проверить свои сети и определить, было ли у них вторжение.
2. Не разрабатываются Advisories – руководство по противостоянию и реагированию на кибератаки.
3. Не предоставляется помощь по искоренению нарушителей из сетей организаций. А это очень сложный и длительный процесс, который может занять месяцы, и требующий методологической поддержки.
4. Госспецсвязь должна дать организациям инструменты, которые позволят им понять, скомпрометированы ли их сети, а также обучить организации реагировать на кибератаки.

Госспецсвязь должна анализировать образцы хакерских инструментов с недавних атак, и публиковать руководства по поиску признаков вторжения, противостояния и искоренения хакеров, как это делают за рубежом.

Государство должно помогать организациям готовиться к атакам, а также помогать проводить сдерживание и искоренение злоумышленников из компьютерных сетей организаций, которые подверглись атаке, а также необходима система управления, которая позволит централизованно оперативно руководить действиями уполномоченных силовых структур (Армия, Полиция, Госспецсвязь, СБУ) в случае кибератак, а также привлекать волонтеров и бизнес, если нужна поддержка.

Литература

1. Яновский А. Проблемы в сфере кибербезопасности в Украине [Електронний ресурс] / Алексей Яновский // Украинская правда. – 2017. – Режим доступу до ресурса:http://www.pravda.com.ua/rus/columns/2017/02/15/7135442/.

Коновалов С.А.
студент кафедры Телекоммуникационных систем и сетей
Государственный университет телекоммуникаций
г. Киев, Украина

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ КОМПАНИИ ОТ ВРЕДОНОСНОГО КОДА

В настоящее время во многих компаниях бытует распространённое мнение о том, что для эффективной защиты АС от вредоносного ПО достаточно установить антивирусные продукты на всех рабочих станциях и серверах, что автоматически обеспечит нужный уровень безопасности. Однако, к сожалению, практика показывает, что такой подход не позволяет в полной мере решить задачу защиты [1] от вредоносного кода. Обусловлено это следующими основными причинами:

1. Подавляющее большинство антивирусных средств базируется на сигнатурных методах выявления вредоносного ПО, что не позволяет им обнаруживать новые виды вирусов, сигнатуры которых отсутствуют в их базах данных;
2. В ряде случаев в организациях отсутствуют нормативно-методические документы, регламентирующие порядок работы с антивирусными средствами защиты. Это может приводить к возможным нарушениям правил эксплуатации, а именно - несвоевременному обновлению сигнатурных баз, отключению компонентов антивирусов, запуску программ с непроверенных информационных носителей и т.д.
3. Антивирусные средства защиты не позволяют выявлять и устранять уязвимости, на основе которых компьютерные вирусы могут проникать в АС предприятий;
4. Антивирусы не обладают функциональными возможностями, позволяющими ликвидировать возможные последствия вирусных атак;
5. Персонал компании зачастую не осведомлён о возможных вирусных угрозах, вследствие чего допускаются непреднамеренные ошибки, приводящие вирусным атакам;

Для того, чтобы избежать перечисленных выше недостатков рекомендуется использовать комплексный подход, предусматривающий возможность одновременного применения организационных и технических мер защиты от вирусных угроз.

Литература

1. Сердюк В. Комплексный подход к защите компании от вредоносного кода [Електронний ресурс] / Віктор Сердюк // №19. – 2008. – Режим доступу до ресурсу: http://www.klerk.ru/soft/articles/73546/.

Коновалов С.А.
студент кафедры Телекоммуникационных систем и сетей
Государственный университет телекоммуникаций
г. Киев, Украина

КИБЕРБЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ

Пример с «PETYA.A» наглядно продемонстрировал, что угроза кибератак сегодня весьма реальна и может коснуться каждого. Большая часть актов киберпреступности приходится именно на банки и остается вне статистики. Банки, в первую очередь, не заинтересованы в разглашении подобной информации, поскольку даже слухи об этом могут дискредитировать их в глазах клиентов, что повлечет значительный отток капитала. В то же время, по причине киберпреступности, банки теряют миллиарды долларов ежегодно.

По прогнозам экспертов, в 2017 году число кибератак на финансовые учреждения увеличится практически на треть по сравнению с прошлым годом. Обусловлено это, с одной стороны, все более стремительным развитием технологий, а с другой тем, что банки и финансовые организации по-прежнему недооценивают риски и масштабы проблемы.

Вместе с тем, реалии таковы, что сегодня хакерских атак совершается во много раз больше, чем других видов экономических преступлений, а их расследованием занимается ограниченное количество специалистов. Вместе с тем имущественный ущерб от киберпреступлений куда выше, чем от других видов преступлений.

Основоположные причины киберугроз можно разделить на несколько групп:

1. отсутствие необходимого законодательства и единых стандартов безопасности
2. недостаточность финансирования со стороны самих банков
3. отсутствие корпоративной культуры в сфере кибербезопасности внутри банка.

Литература

1. Данилов В. КИБЕРБЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ [Електронний ресурс] / Виктор Данилов. – 2017. – Режим доступу до ресурса: https://icf.ua/blog/view/kiberbezopasnost-v-bankovskoy-sfere

Сушко Д.О.
студент кафедры Телекоммуникационных систем и сетей
Государственный университет телекоммуникаций
г. Киев, Украина

ПРИНЦИПЫ ЗАЩИТЫ ИНТЕРНЕТА ВЕЩЕЙ

Анализ ситуации показывает необходимость использования комплексного и научно-обоснованного подхода к обеспечению безопасности Интернета вещей:

1. Оценка рисков – для разработчика важно понимать все потенциальные уязвимости. Методология оценки должна охватывать вопросы обеспечения конфиденциальности, безопасности, предотвращения мошеннических действий, кибератак и кражи интеллектуальной собственности. Оценка рисков отнюдь не является простой задачей, поскольку киберпреступники находятся в постоянном поиске и постепенно осваивают всё новые и новые виды угроз. И поскольку универсального решения для нейтрализации этих угроз не существует, на этом этапе рекомендуется пригласить для консультаций эксперта в области безопасности.
2. Обеспечение безопасности на этапе проектирования – ключевой момент заключается в том, что безопасность устройства должна учитываться на этапе проектирования. Сюда относится безопасность в конечных точках и профилактические меры, в том числе создание защищенного ко взлому аппаратного и программного обеспечения.
3. Обеспечение безопасности данных – строгая аутентификация, шифрование и безопасное управление ключами шифрования должны использоваться для защиты информации, как хранящейся на устройстве, так и в момент её передачи.
4. Управление жизненным циклом – обеспечение безопасности не следует рассматривать как обособленный процесс, который достаточно выполнить один раз и забыть о нём. Крайне важно, чтобы устройства, использующиеся в экосистеме Интернета вещей, были защищены на протяжении всего их жизненного цикла, не важно, идёт ли речь о самостоятельном продукте, или о некой системе.

Литература

1. Совместная безопасность: подход к решению проблем интернет-безопасности [Электронный ресурс] / Internet Society // – 2015. – Режим доступа: https://www.internetsociety.org/collaborativesecurity/.
2. IoT in Financial Services and Banking - Definition and Examples [Электронный ресурс] // – 2016. – Режим доступа: https://www.k-message.com/iot-financiaL-services-bank-marketing-definition-exampLes/.

Поперешняк С.В.
к.ф.-м.н., доц. кафедры Программных систем и технологий
Факультет информационных технологий
Киевский национальный университет имени Тараса Шевченка
Ларченко Ю.С.
студентка кафедры Инженерии программного обеспечения
Учебно-научный институт компьютерных информационных технологий
Национальный авиационный университет
г. Киев, Украина

ТЕХНОЛОГИЯ СКАНИРОВАНИЯ РАДУЖКИ ГЛАЗА В РАМКАХ INTERNET OF EVERYTHING

Перспективой создания Internet of Everything (IoE) является создание распределенной вычислительной среды, которую называют fog computing, что можно переводить как "компьютерный туман". На сегодняшний день достаточно часто рассматривается разработка любых исполнительных устройств, которые преображают команды вычислительной среды IoT в действия в физическом мире. Например, выдача корма домашнему животному, краны, которые определяют необходимый объем воды для мытья предметов[1].

В IoE задействуются встроенные средства идентификации в различные объекты - распознаваемые метки. Например, распознание рисунка на сетчатке глаза или его радужке.

Технологии распознавания радужной оболочки глаза становятся все более популярными во всем мире и используются многими коммерческими и правительственными учреждениями для различных целей, например, для системы контроля доступа (СКД) [2].

Сетчатка, в отличии от радужной оболочки глаза, состоит из фоторецепторных клеток, расположенных на задней стенке глаза, и ее нельзя увидеть. В то время как при распознавании радужной оболочки, в сущности, фиксируется рисунок текстуры радужки, при сканировании сетчатки глаза захватывается изображение сетки кровеносных сосудов внутри глаза [3].

Американская компания Iris ID, что находится в штате Нью-Джерси, выпускает программное обеспечение для распознавания радужной оболочки глаза с 1999 года.

Процесс распознавания личности с помощью радужной оболочки глаза можно условно разделить на три основных этапа: получение цифрового изображения, сегментация и параметризация.

Процесс аутентификации начинается с получения детального изображения глаза человека. Так как радужная оболочка - уникальный параметр, то даже нечёткий снимок даст достоверный результат. Для этой цели используют монохромную CCD камеру с неяркой подсветкой, которая чувствительна к инфракрасному излучению [4-5]. Обычно делают серию из нескольких фотографий из-за того, что зрачок чувствителен к свету и постоянно меняет свой размер. Серия снимков делается буквально за несколько

секунд. Затем из полученных фотографий выбирают одну или несколько и приступают к сегментации.

Сегментация занимается разделением изображения внешней части глаза на отдельные участки (сегменты). В процессе сегментации на полученной фотографии прежде всего находят радужную оболочку, определяют внутреннюю границу (около зрачка) и внешнюю границу (граница со склерой). После этого находят границы верхнего и нижнего века, а также исключают случайное наложение ресниц или блики. После определение границ изображение радужки необходимо нормализовать. В частных случаях нормализация представляет собой переход в полярную систему координат (Полярная система координат — двухмерная система координат, в которой каждая точка на плоскости однозначно определяется двумя числами — полярным углом и полярным радиусом. Полярная система координат особенно полезна в случаях, когда отношения между точками проще изобразить в виде радиусов и углов). После нормализации при помощи псевдо-полярных координат выделенная область изображения переходит в прямоугольник, и происходит оценка радиуса и центра радужки.

В ходе параметризации радужной оболочки из нормализованного изображения выделяют контрольную область. К каждой точке выбранной области применяют двумерные волны Габора (можно применять и другие фильтры, но принцип остаётся таким же) для того, чтобы извлечь фазовую информацию (Фильтр Габора — линейный электронный фильтр, импульсная переходная характеристика которого определяется в виде гармонической функции, помноженной на гауссиан. При цифровой обработке изображений этот фильтр применяется для распознавания границ объектов).

Несомненным плюсом фазовой составляющей является то, что она, в отличии от амплитудной информации не зависит от контраста изображения и освещения. Полученная фаза обычно квантуется 2 битами. Итоговая длина описания радужной оболочки, таким образом, зависит от количества точек, в которых находят фазовую информацию, и количества битов, необходимых для кодирования. В итоге получают шаблон радужной оболочки, который побитно будет сверяться с другими шаблонами в процессе аутентификации. Мерой, с помощью которой определяется степень различия двух радужных оболочек, является расстояние Хэмминга (Расстояние Хэмминга — число позиций, в которых соответствующие символы двух слов одинаковой длины различны. В более общем случае расстояние Хэмминга применяется для строк одинаковой длины любых q-ичных алфавитов и служит метрикой различия объектов одинаковой размерности).

Достоинством метода является и простота в сканировании. Человеку не обязательно сосредоточенно смотреть в одну точку, ведь пятна на сетчатке находятся прямо на поверхности глазного яблока и легко считываются на расстоянии, не превышающем 1 метр. Использовать данный метод удобно в банковских организациях или общественном транспорте. Первая модель смартфона со сканером радужной оболочки появилась в 2015 году в Японии - Fujitsu Arrows NX F-04G. А в Китае ряд компаний (ZTE CORPORATION)

работает над созданием комбинированных технологий идентификации по сетчатке и радужке.

Литература

1. Аутентификация по радужной оболочке глаза. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/

2. Системы распознавания радужной оболочки глаза для контроля доступа. [Электронный ресурс]. Режим доступа: http://www.worldvision.com.ua/articles/sistemi-raspoznavaniya-raduzhnoy-obolochki-glaza.html

3. Современные методы идентификации по биометрическим показателям. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/311876/

4. From Machine-to-Machine to the Internet of Things. Introduction to a New Age of Intelligence., 2006. [Электронный ресурс]. – Режим доступа: http://www.mforum.ru/news/article/110233.htm

5. What the Internet of Everything really is – a deep dive. [Электронный ресурс]. – Режим доступа: https://www.i-scoop.eu/internet-of-things-guide/internet-of-everything/

Поляков С.А.
к.ф.м..н., доц.кафедры Программных систем и технологий
Киевський национальний университет имени Тараса Шевченко
г. Киев, Украина

ЗАДАНИЕ ИЕРАРХИЧЕСКОЙ МОДЕЛИ ДАННЫХ ДЛЯ ХРАНЕНИЯ СЛАБОСТРУКТУРИРОВАННЫХ ДАННЫХ

Для обеспечения информационной безопасности актуальной является проблема хранения больших обьемов слабоструктурированных данных. В работе задается иерархическая модель данных, которая предназначена для хранения слабоструктурированных данных. Она, фактически, является математической моделью популярного формата JSON, который широко используется в расширениях реляционных баз данных и в NoSQL базах данных. Несмотря на свою распространенность в программных системах, свойства этого формата и операций на нем до сих пор не исследовались.

Построение ведется на основе композиционного подхода к программированию [1]. В свое время он был успешно применен при описании семантики реляционных баз данных и языка SQL [2]. Модель данных является расширением и модификацией модели данных, построенной в [3].

В работе индуктивным образом вводятся определения записей и документов.

По аналогии с отношением включения для множеств, для документов и записей определяются отношения быть поддокументом $\sqsubseteq$ и быть подзаписью, $\preccurlyeq$ которые учитывают внутреннюю структуру документов и записей.

Теорема 1. Отношение $\preccurlyeq$ является отношением предпорядка. Т.е. оно рефлексивно, транзитивно, но не антисимметрично.

Теорема 2. Отношение $\sqsubseteq$ является отношением предпорядка. Т.е. оно рефлексивно, транзитивно, но не антисимметрично.

Литература

1. Редько В. Н. Основания композиционного программирования / В. Н. Редько // Программирование. – 1979. – № 3. – С. 3-13.

2. Редько В.Н. Реляційні бази даних: табличні алгебри та SQL-подібні мови / В.Н. Редько, Ю.Й. Брона, Д.Б. Буй, С.А. Поляков // Київ: Видавничий дім «Академперіодика», 2001. – 196 с.

3. Polyakov S. Formal Specification of the NoSQL Data Model/ S.Polyakov, D. Buy, I. Hryshko// International Conference "INFORMATICS'2013" **(**Slovakia, Spišská Nová Ves, November 5th – 7th, 2013). - P. 284-288

Brazhenenko M. G.
student of Information technology faculty
Bychkov O. S.
candidate of physical-mathematical sciences, assistant professor, head of program system and technologies department
Shevchenko V. L.
doctor (technical sciences), professor, professor of program system and technologies department
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

AUTOMATION OF PUBLICATION AND SUBSCRIPTION IN EMERGENCY CONTROL WIRELESS NETWORKS

The problem of this work has vital origin. Very often seniors suffering from heart attack may not be able to ask for an ambulance. Sometime child (alone at home or out home) may not be able to ask parents for help. Whole list of danger scenarios could be expanded. So, an issue of quick, reliable, simple and friendly way of transferring data about adverse circumstances is actual.

Main research objective: improve operational information quality about adverse events. **Sub-tasks:** 1. Ability to select responsible persons and a way to transfer data. Ability to subscribe for users signals. 2. Providing persons with limited abilities communication interfaces to ask for ambulance. 3. Affordability for vast majority of people.

Additional requirements: 1. Person is able to transfer information. 2. Person understands how to use alarm devices. 3. Affordability and ability to carry everywhere (like watches).

Proposed solution consists of: 1. Web application and services providing connection to recipients with free user preferences deployed to cloud. 2. SMS Gateway receiving SMS messages and resending them to cloud. 3. Station receiving messages from end-user devices and deciding where and what is the right way to resend (directly to cloud or alternatively due to cloud unavailability and other reasons send SMS message to SMS Gateway). 4. Device with Button – reference designation for the end-user device carried and has a button to be pressed at any moment.

Main research directions: 1. Investigation of SMS processing systems – research of ready for usage solutions, able to perform SMS Gateway function. Raspberry PI combined with GSM module founded as an optimal solution. 2. Investigation of available wireless communications with Raspberry PI – a balance were founded for bandwidth and range between connected devices. Lora and LoRaWan stack and modules for embedded systems founded as the best option. 3. Specification of the protocol for message exchange – Bandwidth is a concern for radiowaves based modules and as a result decided to analyze existing protocols for instant messaging and taken optimal decision between new and existing protocols.

Organizing of optimal message exchange require specific protocol, (existing one or developed). For optimal decision next actions performed: 1. Elaborated system of criteria for instant messaging protocols valuation. 2. Evaluated protocols by system of criteria. Conclusion taken about possible improvements of achieved valuation results.

Shevchenko V.
doctor (technical sciences), professor, professor of program system and technologies department
Taras Shevchenko National University of Kyiv
Shcheblanin J.*, *Shevchenko A.
State University of Telecommunication
Kyiv, Ukraine

THE EPIDEMIOLOGICAL APPROACH TO PROGNOSIS AND MANAGEMENT OF INFORMATION INCIDENTS OF INTERNET OF EVERYTHINGS

In 2012, Cisco introduced the concept of Internet of Everything (IoE) [1], as an aggregation of **people, processes, data and things**, which increases the value of network connections to unprecedented levels. By 2020, more than 50 billion different devices, that generate zettabytes of cloud-based data [2], will be connected via wired and wireless networks to the Internet. But this indicator does not include sensors [3]: in 2012, worldwide, there were 2 billion sensors, in 2013 - 8 billion, in 2015 - 24 billion. Development opportunities are enormous, because 99.4% of physical objects, that are capable of becoming IoE objects, are still not connected to the Web [4]. The rate of IoE proliferation is increasing. By 2020, the number of "smart" things in the world exceeds the number of smartphones and PCs and will equal 25 billion devices. According to Cisco, [5], in the next decade, thanks to the unconnected subscription, IoE can provide the private sector of the world economy with a profit of about 14.4 trillion US dollars.

But, as steadily as the Internet grows in the form of IoE, the number of incidents of information and cyber security is increasing. The greater the value created by the Metcalfe law, the more opportunities cybercriminals and their malicious software receive. With an increase in the number of links in the network, the similarity of the laws of cybernetic attacks to the laws of the development of biological and medical epidemics increases.

Action algorithms of biological viruses are similar to algorithms of computer viruses. For prevention of biological virus intrusion, usually use vaccination. At same way for prevention of computer viruses intrusion, usually use antivirus. In both of cases we have so called “zero day threats” when type of virus is unknown. Therefore prevention means are unknown too. In this case we defend our body (computer of biological) from “Diseases of dirty hands”. By another words, common sanitary rules may protect us from infection.

The intensity of the attacks and the consequences need to be predicted for the effective counter attacks. So study of forecasting models of information and cyber-attacks is **relevant**. The results of the study of biological epidemics regularities accumulated centuries and can be useful for predicting the consequences of information and cyber-attacks.

The **purpose of the article** - use the experience of mathematical modeling of biological epidemics [6], to predict the results of large-scale information and cyber-attacks.

Exponential growth with saturation models used in processes that have reached the limit of its development. If the resource provision varies randomly or seen several stages of the life cycle, it is more adequate the S-shaped logistic model [7, 8] $y(t) = Y_{min} + \frac{Y_{max} - Y_{min}}{1 + e^{-m \cdot (Y_{max} - Y_{min}) \cdot (t - \Delta t)}}$. Here y - dynamic development variable (eg, infected); t - time; Y_{min}, Y_{max} - lower and upper limits of y values; m - a permanent factor; Δt - abscissa of symmetry point (shift along the abscissa axis). Similar models are used to simulate the dynamics of growth of infection by computer viruses. Dynamics models of virus spread (SI, SIS, SIR, AAWP, PSIDR) take into account specific of distributed environment (computer network topology) and specifics of combating against the viruses [9, 10]. Integral-differential equations are most appropriate for epidemics simulate [11, 12]. The result of solving these equations is the family of S-shaped curves and curves resulting additive convolution the latter.

Modifies the known structural Boyev-model (Fig.1) [11]. Let: P - the total number of infected sites, S, N - susceptible and resistant to infection, E - in incubation (infected themselves, but have not infect others and not identified), I - contaminated sites that are actively infect others, R - objects that are treated and received immunity (antivirus), F - items that had to be completely removed from work after infection; K_s, K_E, K_F - coefficients susceptibility to infection, transmission of infection, withdrawal from work (total disability); $f(I,S,K_E)$ - logistical dependence of infection among susceptible.

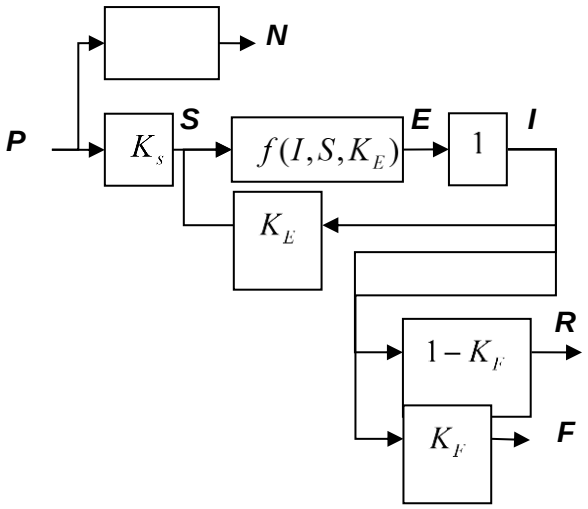


Fig.1. The modified structural epidemic model by Boyev

Implementation of the model proved its efficiency and adequacy (Fig.2). Timeline is different for different types of information and cyber-attacks. The main attention is given for multi-layered attacks. Therefore, in the model were saved purely biological characteristic - the incubation period. The incubation period in the computer world correspond the latent period during which the malicious code executes additional adjustment, additional penetration in complete secrecy of their actions. In multi-level attack malicious code type 1 initially weakened defense, prepares virtual channels guaranteed access to information resources and resource management in future. Then, by well-prepared channels malicious code type 2 enters the system (or in another more secure or more controlled part of system) and perform

basic tasks malware. Such attacks levels may be several. These levels can combine different attacks ways from highly technical to social engineering.

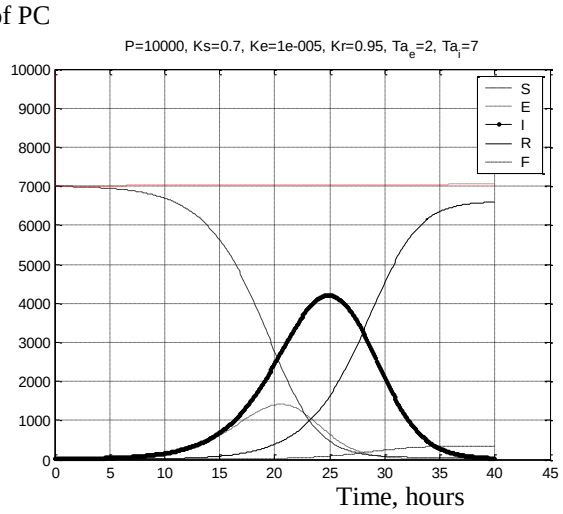


Fig.2. The results of numerical simulation of a cyber-attack.

The graphs show the logistics nature of reducing the number of favorable sites and the increasing number of cured objects and objects removed from work. General view of the number of infected objects and objects that are in the incubation period corresponds to existing statistical data on the development of biological epidemics, allowing the use of known biological laws for the computer world. The main practical result of simulation is a useful "bell"- dependence of the number of infected objects. Amplitude of this dependence determines the level of epidemic danger. This is fundamental epidemics difference in biological and computing world. In the computer world is dangerous, any infection. .

If we know dangerous level of epidemic peak, then we can provide some limitation (control) for ratios K_s and K_E. Appropriate values of K_s and K_E will provide non-dangerous epidemic peak level in incidents case. In this meaning K_s and K_E is guidance for information and cyber incidents epidemic process.

The logistic model adequately predicts the epidemic and allows you to schedule regular proactive measures. A great feature of the model is complete visibility of the physical variables and all mathematical transformations. This allows you to accurately monitor the adequacy of the model and make the necessary adjustments in time. New result is separation of data on the number of infected objects and objects that are in the incubation period for the temporal stages corresponding states. This provides additional opportunities for disease control measures.

References

1. Dave Evans. How the Internet of Everything Will Change the World…for the Better #IoE [Infographic] // Blog of Dave Evans. https://blogs.cisco.com/digital/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic

2. *Стюарт Тейлор (Stuart Taylor)* Сервис-провайдеры могут возглавить внедрение технологий Всеобъемлющего Интернета https://www.cisco.com/c/ru_ru/about/press/press-releases/2014/12-121914a.html

3. Мэтью Смит (Matthew Smith). Всеобъемлющий Интернет: нужно быть готовым к изменениям. 1.10.2015. https://glavportal.com/materials/vseobemlyushchiy_internet_nuzhno_byt_gotovym_k_izm/

4. Владимир Зотов. Internet of What? В чем на самом деле разница между M2M, IoT и IoE. 23.09.2016. https://www.billing.ru/blog/internet-what

5. Джозеф Бредли. Всеобъемлющий Интернет на весах ценности для частного бизнеса. 04 июля 2013. http://www.iksmedia.ru/articles/4951514-Vseobemlyushhij-Internet-na-vesax.html

6. Shevchenko A.V., Gepko A.L. (2011) "Matematychna model prognozuvannja dynamyky epidemij" [Mathematical model of epidemics dynamics prognosis], Prophylactics medicine, no.3(15), pp.3-6.

7. Shevchenko A.V., Shevchenko V.L (2010) "Grubi modeli rozvitku v medycyni" [Rough development models in medicine], Medical informatics and engineering, no.4, pp. 52-55.

8. Shevchenko V.L. (2011), "Optymizacijne modeljuvannja v strategichnomu planuvanni" [Optimizing modeling in strategy planning], Kiev.: CVSD NUOU. – 283 p.

9. Monahov Yu.M., Hruzdeva L.M. and Monahov M.Yu. (2010) "Vredonosnye programy v kompjuternych setjach" [Malicious software in computer networks]: Textbook. Vladymyrskyy state.univ. - Vladimir: Publishing House Vladym.state univ. Press. 72p.

10. Klymentiev K.E. (2013) "Kompjuternye virusy s antivirusy: vzgljad programmista" [Computer viruses and antiviruses: programmers view], - Moskow: DMK Press. 656 p.

11. Boev B.V. (2017). "Kompjuternoe modelirovanie v ocenke posledstvij akta biologicheskogo terrorizma" [Computer modeling in evaluation of the aftermath of the biologically terrorism act], in Proceedings. I Russian Symposium on biological security. - Moscow: Research institute of Epidemiology and Microbiology named by Gamaleia N.F. RAMS. Available at: www.bio.su. (accessed 23 March 2017)

12. Shevchenko V., Shevchenko A. (2017) The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems. 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Polyana, 2017 April 20-23, pp.174-177. http://ieeexplore.ieee.org/document/7937561/ DOI: 10.1109/MEMSTECH.2017.7937561

Antonyuk O.
student of Information technology faculty
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

IoE FOR THE PUBLIC SECTOR

IoE's ability to connect ever-growing numbers of sensors and actuators to objects or things on the Internet, to extract and analyze growing amounts of useful data, and then to use that analysis in automated and people-based processes has enormous potential across all sectors.

More than perhaps any technological advance since the dawn of the Internet, the Internet of Everything – the networked connection of people, process, data, and things – holds tremendous potential for helping public-sector leaders address their many challenges, including the gap currently separating citizen expectations and what governments are actually delivering

IoE-driven benefits from programs such as connected transportation, smart roads, social care, and education accrue as reductions in overall costs, especially through better targeting and control of resource usage. Other programs have indirect benefits for government – economic, social, or environmental – but direct benefits for citizens and businesses in terms of reduced transactional costs and time saved, or in external benefits such as better quality of life. Researchers at Harvard University have identified whole system impacts of smart road systems that go beyond shorter journey times and reduced traffic congestion to also promote better land use as car parking space is used more efficiently – eventually resulting in reduced pressure on urban land use and, hence, lower housing costs.

At the city level, the integration of technology and quicker data analysis will lead to a more coordinated and effective civil response to security and safety (law enforcement and blue light services); higher demand for outsourcing security capabilities. At the building level, security technology will be integrated into systems and deliver a return on investment to the end-user through leveraging the technology in multiple applications.

There will be an increase in the development of "Smart" vehicles which have low (and possibly zero) emissions. They will also be connected to infrastructure. Additionally, auto manufacturers will adopt more use of "Smart" materials. The key focus will be to make the city smarter by optimizing resources, feeding its inhabitants by urban farming, reducing traffic congestion, providing more services to allow for faster travel between home and various destinations, and increasing accessibility for essential services. It will become essential to have intelligent security systems to be implemented at key junctions in the city. Various types of sensors will have to be used to make this a reality. Sensors are moving from "smart" to "intelligent".

References

1. Consumer Goods Forum, 'Rethinking the Value Chain: new realities in collaborative business'
2. SeeDiscover, 'Behind The Numbers: Growth In The Internet Of Things'
3. Ovidiu Vermesan, 'Digitising the_Industry IoT'

Palamarchuk E.
student of Information technology faculty
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

IoE ECONOMY

To get the most value from IoE, business leaders should begin transforming their organizations based on key learnings from use cases that make up the majority of IoE's Value at Stake. The most important facts of the IoE and economy connection:

• The Internet of Everything (IoE) creates $14.4 trillion in Value at Stake – the combination of increased revenues and lower costs that is created or will migrate among companies and industries from 2013 to 2022.

• The five main factors that fuel IoE Value at Stake are: 1) asset utilization (reduced costs) of $2.5 trillion; 2) employee productivity (greater labor efficiencies) of $2.5 trillion; 3) supply chain and logistics (eliminating waste) of $2.7 trillion; 4) customer experience (addition of more customers) of $3.7 trillion; and 5) innovation (reducing time to market) of $3.0 trillion.

• Technology trends (including cloud and mobile computing, Big Data, increased processing power, and many others) and business economics (such as Metcalfe's law) are driving the IoE economy.

• These technology and business trends are ushering in the age of IoE, creating an unprecedented opportunity to connect the unconnected: people, process, data, and things. Currently, 99.4 percent of physical objects that may one day be part of the Internet of Everything are still unconnected.

• To get the most value from IoE, business leaders should begin transforming their organizations based on key learnings from use cases that make up the majority of IoE's Value at Stake. These use cases include smart grid, smart buildings, connected healthcare and patient monitoring, smart factories, connected private education, connected commercial (ground) vehicles, connected marketing and advertising, and connected gaming and entertainment, among others.

• Robust security capabilities (both logical and physical) and privacy policies are critical enablers of the IoE Economy. The IoE Value at Stake projections are based on increasingly broad adoption of IoE by private-sector companies over the next decade. This growth could be inhibited if technology-driven security capabilities are not combined with policies and processes designed to protect the privacy of both company and customer information.

Challenges abound for today's business leaders. The rapid pace of change creates confusion and misinformation, which often leads to poor decision making or, worse, inaction. When combined with price transparency and global supply chains, many of the same technology trends that are ushering in the IoE era are also enabling new entrants to become viable threats in just weeks and months rather than years. In this environment, winners and losers are determined faster than ever before. With $14.4 trillion Value at Stake, IoE presents an important opportunity to increase market share, gain competitive advantage, strengthen and grow your customer base, and increase profitability. And because the stakes are high — over 10 years, companies stand to lose more than a year of profits if they do not embrace IoE — the time to act is now.

Ptushkin S.
student of Information technology faculty
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

INTERNET OF THINGS: INTERCROSSING TECHNOLOGIES FOR INTELLIGENT ENVIRONMENTS AND INTEGRATED ECOSYSTEMS

In order to enable a fast uptake of the IoT, key issues like identification, privacy and security and semantic interoperability have to be tackled. The interplay with cloud technologies, big data and future networks like 5G have also to be taken into account.

In this context the new concept of Internet of Energy requires web based architectures to readily guarantee information delivery on demand and to change the traditional power system into a networked Smart Grid that is largely automated, by applying greater intelligence to operate, enforce policies, monitor and self-heal when necessary. This requires the integration and interfacing of the power grid to the network of data represented by the Internet, embracing energy generation, transmission, delivery, substations, distribution control, metering and billing, diagnostics, and information systems to work seamlessly and consistently.

This concept would redefine solving the problem and enable the ability to produce, store and efficiently use energy, while balancing the supply/demand by using a cognitive Internet of Energy that harmonizes the energy grid by processing the data, information and knowledge via the Internet.

The Internet of Energy will leverage on the information highway provided by the Internet to link computers, devices and services with the distributed smart energy grid that is the freight highway for renewable energy resources allowing stakeholders to invest in green technologies and sell excess energy back to the utility.

The imitational model proves that this development of smart entities will encourage development of the novel technologies needed to address the emerging challenges of public health, aging population, environmental protection and climate change, conservation of energy and scarce materials, enhancements to safety and security and the continuation and growth of economic prosperity.

References

1. Vermesan, Ovidiu; Friess, Peter (2013). Converging Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4.
2. Raggett, Dave (27 April 2016). "Countering Fragmentation with the Web of Things: Interoperability across IoT platforms"