МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»
ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА БЕЗПЕКИ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

РАДА МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

X ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

22 листопада 2018 р.

м. Дніпро

УДК [004+621.39](06)
І 74
ББК 32.973

Оргкомітет конференції:

Голова:	Декан факультету інформаційних технологій, д.т.н., професор Алексєєв М.О.
Заступник голови:	Заступник декана факультету інформаційних технологій, ст. викл. Мєшков В.І.
Члени оргкомітету:	д.т.н., професор Корнієнко В.І. к.ф.-м.н., професор Гусєв О.Ю. к.т.н., доцент Флоров С.В. к.т.н., доцент Галушко О.М. ст. викл. Войцех С.І. ст. викл. Кручинін О.В. ст. викл. Тимофєєв Д.С.

І 74

Інформаційні технології. Безпека та зв’язок: Матеріали всеукр. наук.-практ. конф. – Дніпро: НТУ «Дніпровська політехніка», 2018. – 70 с. – (укр. м., рос. м., англ. м.).

Викладено тези доповідей учасників X Всеукраїнської науково-практичної конференції «Інформаційні технології. Безпека та зв’язок», яка відбулася у НТУ «Дніпровська політехніка» 22 листопада 2018 року.

На конференції було розглянуті найбільш актуальні проблеми розвитку інформаційних технологій, безпеки та зв’язку в Україні та шляхи їх вирішення.

УДК [004+621.39](06)
ББК 32.973

ЗМІСТ

Секція 1 – Інформаційні технології

УДК 004

Кобзарь К.О. студентка групи 125м-17-2
Науковий керівник: Мілінчук Ю.А., асистентка кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

АНАЛІЗ ДЕЯКИХ ВЛАСТИВОСТЕЙ ПОШТОВИХ КЛІЄНТІВ MICROSOFT OUTLOOK EXPRESS, THE BAT!, MOZILLA THUNDERBIRD ТА OPERA MAIL

Електронна пошта – служба Інтернету, яка дозволяє її користувачам обмінюватися повідомленнями.

Для користування електронною поштою необхідно мати поштову скриньку на одному із поштових серверів мережі.

Для роботи з поштовою скринькою існують спеціальні онлайнові програми, що мають спеціальний веб-інтерфейс.

Онлайнові програми зручні при невеликих об'ємах листування і менш зручні, коли пошти багато (це характерно частіше для підприємств, закладів, фірм тощо). В такому випадку доцільно використовувати спеціальні програми – поштові клієнти.

ФУНКЦІЇ ПОШТОВОГО КЛІЄНТА

Великі поштові програми, так звані «все в одному», такі як Mozilla Thunderbird, The Bat! і Microsoft Outlook, Opera Mail сьогодні аналізують операції та процеси, які відбуваються у користувача поштового клієнта. Простіші поштові агенти наприклад Mutt, також є поштовими програмами.

На відміну від поштового сервера, клієнт електронної пошти зазвичай відправляє повідомлення не прямо на відповідний сервер одержувача, а на один і той же поштовий сервер, який виступає як релей. Зазвичай це поштовий сервер провайдера або компанії. Відправка пошти найчастіше здійснюється за протоколом SMTP(Simple Mail Transfer Protocol) [1].

Клієнт електронної пошти приймає пошту з одного або декількох поштових серверів, часто це той же сервер, котрий слугує для відправки. Прийом пошти зазвичай здійснюється за протоколами POP(Post Office Protocol) або IMAP(Internet Message Access Protocol).

Також в функції клієнта електронної пошти може входити: сортування, зберігання повідомлень, пошук по архіву повідомлень, ведення адресної книги, фільтрація прийнятих повідомлень за різними критеріями, конвертація форматів, шифрування, організація інтерфейсів з офісними програмами та інші функції.

ВЛАСТИВОСТІ ПОШТОВИХ КЛІЄНТІВ

1. Microsoft Outlook Express - Microsoft Outlook - персональний інформаційний менеджер з функціями поштового клієнта і Groupware компанії Microsoft.

Крім функцій поштового клієнта для роботи з електронною поштою, Microsoft Outlook є повноцінним органайзером, що надає функції календаря, планувальника завдань, записника і менеджера контактів. Крім того, Outlook дозволяє відстежувати роботу з документами пакету Microsoft Office для автоматичного складання щоденника роботи.

2. The Bat! - The Bat! - програма для роботи з електронною поштою для ОС Windows. Розробляється молдавською компанією Ritlabs. Має багато можливостей для сортування листів, а також володіє системою для підключення додаткових модулів розширення (плагінів), призначених для захисту від спаму і вірусів. Як правило, плагіни можна завантажити з сайту розробників подібних модулів. У програмі є вбудований диспетчер пошти для POP3 серверів.

3. Mozilla Thunderbird - безкоштовна кроссплатформенная вільно поширювана програма для роботи з електронною поштою і групами новин, а при установці розширення Lightning і з календарем. Є складовою частиною проекту Mozilla. Підтримує протоколи: SMTP, POP3, IMAP,[2]. Надаються офіційні збірки для Microsoft Windows, macOS, Linux (i386), причому набір можливостей на всіх платформах однаковий. Існують також сторонніх збірок для FreeBSD, Solaris , OpenSolaris, OS / 2.

4. Opera Mail - (стара назва M2) - клієнт електронної пошти і новинний клієнт, раніше вбудований в браузер Opera, а тепер є окремою поштовою програмою. Його інтерфейс трохи відрізняється від інших поштових клієнтів з метою забезпечення кращої інтеграції з Opera. У ньому є фільтри спаму (автоматичний), підтримка протоколів POP3, IMAP, SMTP новинних груп, новинних стрічок RSS, Atom і NNTP.

ВИСНОВОК

Отже, електронна пошта здатна замінити собою безліч факсів і звичайну поштову доставку; електронна пошта набагато дешевше, ніж звична паперова пошта і при цьому забезпечує практично майже миттєві комунікації. Чим більш доступним стає Інтернет, чим вище якість з'єднання і менше сума, яку кожен з нас викладає за користування мережею, тим частіше користувачі користуються web-інтерфейсом для роботи з поштою. Для платформи Windows найбільш популярними поштовими клієнтами є системи:

- Microsoft Outlook Express;
- Opera Mail;
- Mozilla Thunderbird;
- The Bat!

ПЕРЕЛІК ПОСИЛАНЬ

1. Лучшие бесплатные почтовые клиенты для Windows [Електронний ресурс] : http://pcfaq.info/soft/luchshie-besplatnye-pochtovye-klienty-dlja-windows.html ;
2. Жуков Владимир Последняя почта; Современник - Москва, 2017. - 400 с.

УДК 004.588

Машевський А.М. студент гр. ПІт-15-1
Науковий керівник: Сироткіна О.І., доцент кафедри «Програмне забезпечення комп'ютерних систем»
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛЬНОЇ, ДОПОВНЕНОЇ ТА ЗМІШАНОЇ РЕАЛЬНОСТІ В ОСВІТІ

В роботі розглянуті технології віртуальної, доповненої та змішаної реальності, а саме: переваги і недоліки, приклади їх застосування в освіті.

З кожним роком технології віртуальної, доповненої та змішаної реальності стають дедалі доступнішими для придбання. Раніше використовувати такі технології могли тільки великі компанії для навчання своїх підлеглих. Це були великі за розмірами, з'єднані купою дротів з комп'ютером тяжкі шоломи, але тепер все змінилося і їх може використовувати навіть дитина.

За даними психологів, людина сприймає близько 10% інформації, яку вона чує, 30% яку бачить та 90% від того, що вона робить. Саме технології віртуальної реальності дозволяють «робити». Вони здібні на все: проведення фізичних або хімічних випробувань, заміна читання підручників з історії дивовижною віртуальною подорожжю давнім Римом, або учні можуть прослухати матеріал у виконанні вчителя, а потім надягти шолом і в ньому розглядати зображення кровоносної системи, очного яблука, легені, серця та інші. Сучасні програмні забезпечення для освіти за допомогою віртуальної реальності оснащені системою підказок, які будуть допомагати Вам. Це значно спрощує процес навчання.

На жаль, заклади освіти не мають усіх приладів, які потрібні для проведень лабораторних робіт з фізики, хімії та інших предметів. За допомогою віртуальної реальності ми можемо отримати віртуальну лабораторію зі всіма необхідними приладами та нескінченними реагентами.

Технології віртуальної реальності – це не тільки сучасне та цікаве рішення для навчання в освітніх закладах, вони можуть використовуватись на підприємствах для проведення переатестацій, тренувань з пожежної безпеки, або для навчання персоналу роботи зі станками.

Технології віртуальної реальності розподіляються на віртуальну, доповнену та змішану реальність.

Віртуальна реальність – це коли користувач повністю «занурюється» у віртуальний світ, який повністю замінює собою реальний. Для цього використовують спеціальні шоломи, які під'єднуються до комп'ютера або телефона, з якого проеціюється згенероване тривимірне зображення.

Віртуальна реальність хоча і зручна технологія для освіти, але вона має свої переваги та недоліки.

Переваги використання технології віртуальної реальності:

• Наочність. 3D-графіка дозволяє відтворити деталізацію навіть найскладніших процесів, невидимих людському оку, навіть розпад ядра атома або хімічних реакцій. До того ж ніщо не заважає збільшити рівень деталізації і побачити рух електронів або відтворити механічну модель, наприклад, розвитку клітини людського організму на різних етапах. Віртуальна реальність дозволяє відтворити або змоделювати будь-які процеси або явища, про які знає сучасна наука.

• Безпека. Практичні основи управління літальними або надшвидкісними апаратами можна абсолютно безпечно відпрацювати на пристрої віртуальної реальності. Також віртуальна реальність дає можливість відпрацьовувати надскладні медичні операції або маніпуляції без шкоди і небезпеки для кого-небудь.

• Залучення. Технології віртуальної реальності дають можливість змоделювати будь-яку механіку дій або поведінку об'єкта, вирішувати складні математичні завдання в формі гри

та інше. Віртуальна реальність дозволяє подорожувати в часі переглядаючи основні сценарії важливих історичних подій або побачити людину зсередини на рівні руху еритроцита в крові.

• Фокусування. Простір, змодельований в віртуальній реальності, можна легко розглянути в панорамному діапазоні 360 градусів не відволікаючись на зовнішні чинники.

До недоліків використання цієї технології, окрім високої ціни (якщо купувати серйозну техніку), можна віднести те, що при довгому використанні, через розлад органів чуття можливе запаморочення та дезорієнтація після «виходу» з віртуального світу.

Доповнена реальність – це накладення віртуального світу на реальний за допомогою спеціальних шоломів, окулярів, або звичайного смартфону. Таким чином ми можемо одночасно взаємодіяти і з віртуальним, і з реальним світом природним чином.

Доповнена реальність так само, як і віртуальна, може використовуватись в освітніх закладах. За допомогою окулярів додаткової реальності можна подивившись на схему, оснащену спеціальними маркерами, та розглянути її тривимірну проекцію, або те саме можна зробити використовуючи мобільний додаток.

Переваги використання технології доповненої реальності:

• Можливість показати те, що не можна уявити звичними способами.

• Легкість у використанні. Вам не обов’язково потрібні великі шоломи, ви можете використовувати спеціальні окуляри, або звичайний смартфон, завантаживши на нього спеціальний мобільний додаток.

• Можливість «приміряти» віртуальні об'єкти до реального оточення, не виходячи з дому.

До недоліків використання цієї технології можна віднести тільки занадто високу ціну на спеціальні окуляри.

Змішана реальність поєднує в собі віртуальну і доповнену реальність, дозволяючи не тільки бачити віртуальні об’єкти у реальному світі, але і взаємодіяти з ними. Цю технологію можна назвати розширеною версією доповненої реальності з максимально реалістичними об’єктами та можливістю взаємодії з ними.

На даний момент не так багато освітнього програмного забезпечення для віртуальної, доповненої та змішаної реальності, але це технології, які дуже швидко розвиваються, та у недалекому майбутньому можуть стати невід’ємною частиною нашого життя.

ПЕРЕЛІК ПОСИЛАНЬ

1. Что такое VR, AR и смешанная реальность [Електронний ресурс]: https://vc.ru/design/39700-chto-takoe-vr-ar-i-smeshannaya-realnost-sayty-prilozheniya-i-stati-kotorye-pomogut-razobratsya;

2. Виртуальная, дополненная и смешанная реальность: суть понятий и история развития [Електронний ресурс]: https://habr.com/company/dronk/blog/390805/.

УДК 004.827

Панасейко Г.М. студентка гр. ПІіт-15-1
Науковий керівник: Сироткіна О.І., доцент кафедри програмного забезпечення комп'ютерних систем
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ПРОБЛЕМИ ШТУЧНОГО ІНТЕЛЕКТУ, ЯКІ ПРИЗУПИНЯЮТЬ ЙОГО РОЗВИТОК

Штучний інтелект – це програмне забезпечення, яке демонструє можливості аналізу, прийняття рішень і навчання, такі можливості схожі зі здібностями людини. Також, це частина інформатики, яка вивчає інтелектуальні об'єкти не лише з інженерної точки зору. Сьогодні штучний інтелект може бути використаним практично у кожній галузі.

Основними напрямками розвитку інформаційних технологій сьогодні є збір, зберігання та управління інформацією, її представлення та обробка для прийняття рішень. Важливим є не лише отриманий результат, але і методика прийняття рішень. Всі ці операції виконати неможливо без нейронної мережі, яка б дозволила оцінювати попередній досвід і на його основі приймати майбутні рішення.

За останні декілька років розробки в області штучного інтелекту досягли великої популярності. Зараз штучний інтелект використовується в усіх областях від ігор до медицини. Проте, технологія ще недостатньо вивчена. Дуже складно сказати, як саме працює штучний інтелект, а його потенціал викликає сумління у вчених. Для багатьох областей важливе пояснення того, яким чином отриманий результат. Наприклад, у фінансовій сфері нерозуміння того, як саме прийнято рішення нейронною мережею, може призвести до неможливості коректно оцінити ризики стратегій, в медицині неможливо визначити правильність назначеного курсу лікування. Якщо від рішення мережі залежить щось важливе, то будь-яка можлива неадекватність роботи, яка була не поміченою спочатку та на етапі навчання, може мати серйозні наслідки. Внутрішнє представлення результатів такої складної системи може бути проаналізовано з достатньою складністю лише у найпростіших випадках.

Наприклад, нейронна мережа може розрізнити кота від собаки за деякими, відомими лише їй особливостями. Може статися ситуація, коли на явно зображеного кота система приведе до невірної відповіді тому, що знайде непомітні людині особливості зображення і знайде собаку там, де її немає. І навіть, коли в конкретному випадку вдасться помітити помилку і звернути на це увагу при навчанні, все одно невідомо, що може призвести до обману наступного разу. Іноді мережа може навчитися не тому, що передбачалося і замість тварин, визначати результат по фону, який знаходиться за твариною. У той же час, немає методу для точного визначення необхідних параметрів навчання.

Наступною складністю роботи зі штучним інтелектом є те, що йому потрібно в тисячі разів більше інформації, ніж людині, для того, щоб навчитися розрізняти образи. В той час, як дитина може розрізнити тварину чи об'єкт після одної побаченої фотографії. Можна помітити, що використання технології deep learning (глибинного вивчення), має успіх там, де є багато даних. Проблема закладається в тому, що в багатьох областях важко зібрати велику кількість інформації. В таких ситуаціях, єдиним виходом є не лише отримання інформації, а використання алгоритмів, яким потрібно не так багато ресурсів.

Штучний інтелект не пристосований до мультизадачності. Не існує алгоритмів, які можуть виконувати декілька задач. Можна навчити штучний інтелект знаходити котів або визначати ризики стратегій, але це не буде один штучний інтелект. Нейронні мережі на деякому етапі перестають піддаватися обробці через свої розміри. В компанії DeepMind цю проблему називають «катастрофічною забутливістю». Штучний інтелект, отримавши нові алгоритми, «забуває» про попередні для того, щоб звільнити пам'ять для нової інформації.

Можливості штучного інтелекту несуть з собою не лише вигоду, але й наслідки для економіки, політики, безпеки, охорони. Перші переваги технологій уже бачать у багатьох

областях, тому розвиток штучного інтелекту є бажаним і компанії виділяють більше коштів на інвестування у цю сферу. Проте, його впровадження змінить ринок труда та ролі людей. Це кардинально змінить ряд професій людей, де вони ще будуть потрібними. Багато професій просто будуть замінені роботами, і люди залишаться безробітними. Наприклад, уже зараз Google інвестує у роботів, які пишуть новини без участі людини. Деякі види програмістів також можуть залишитися без роботи, і це більше «кодери», які готують готові блоки і їх працю можна звести до алгоритму. Також, це стосується і HR-спеціалістів: нейромережі можуть охоплювати більше джерел інформації, ніж людина для того, щоб шукати кандидатів, систематизувати їх по різноманітним критеріям і відправлять повідомлення.

На жаль, компанії, бажаючі отримати передові технології, можуть забути про ту небезпеку, яка йде від штучного інтелекту. Розвинутий штучний інтелект може бути використаним для впливу на політичне мислення та думки людей. Поступово відповідальність у компаніях переходить від людини до машини. У той же час, це призводить до вразливості автоматизованих, автономних машин чи злим діям, які відносяться до кібербезпеки, а також порушень у роботі і збитків. Крім цього, штучний інтелект може дозволити собі використовувати дрони як зброю, що є прямою загрозою людству.

Можна зробити висновок, що поки що розвиток штучного інтелекту та нейронних мереж має перелік проблем, з якими стискаються розробники та користувачі. Поки вони не будуть вирішені, загроза ризиків буде такою ж великою та може призвести до несправних наслідків.

ПЕРЕЛІК ПОСИЛАНЬ

1. Штучний інтелект: [Електронний ресурс] режим доступу https://uk.wikipedia.org/wiki/.
2. Ryszard S. Michalski, Jaime G. Carbonell, Tom M. Mitchell (1983), Machine Learning: An Artificial Intelligence Approach, Tioga Publishing Company, ISBN 0-935382-05-4.
3. Allianz Global Corporate & Specialty, «Зліт штучного інтелекту: майбутні перспективи і можливі ризики».
4. Іонов С.Д. Розподілена нейронна мережа: принципи роботи і протоколи взаємодії / С.Д. Іонів // Матеріали міжвузівської наукової конференції з проблем інформатики «СПИСОК-2009». - 2009.

Секція 2 – Кібербезпека

УДК 681.518.54

Гречко К.О. студент гр. 125м-17-1
Ковальова Ю.В. аспірант кафедри кібербезпеки та захисту інформації Київського університету імені Тараса Шевченка
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

КРИПТОВАЛЮТА ІОТА ТА ПРИНЦИП ЇЇ РОБОТИ

ІОТА - криптовалюта, розроблена для Інтернету Речей. Вона не схожа ні на один інший проект, що робить її унікальною та багатообіцяючою. ІОТА здатна стати тим транзакційних паливом, яке забезпечить реалізацію розумних підприємств за участю машин, об'єднаних в одну мережу. За словами розробників, вона має велику кількість переваг в порівнянні з блокчейном Bitcoin. Особливо це відноситься до здійснення мікроплатежів (наприклад, одноцентових). ІОТА повністю децентралізована та на відміну від інших криптовалют не має комісій за транзакції. Також у порівнянні з тими ж Bitcoin, де у проведенні транзакції беруть участь користувач та майнер, то тут злшився лише користувач. Щоб провести транзакцію ІОТА, користувачу потрібно підтвердити дві операції від інших користувачів.

Як заявляють розробники ІОТА, вона позбавиться проблем, характерних для інших криптовалют:

- Централізація майнінгу – оскільки майнери схильні об'єднуватися у великі групи, це може призвеси до централізації та можливості реалізації «атаки 51%». Це абсолютно неприпустимо в Інтернеті речей.
- Застаріла криптографія – слід враховувати появлення квантових комп’ютерів у майбутньому.
- Труднощі проведення мікроплатежів – в світі Інтернету речей наявність транзакційних комісій для майнерів і спам-атаки робляться критичними.
- Нетерпимість до поділу – при відокремленні частини від цілої мережі криптовалюти на основі блокчейну не можуть існувати. Також неможливим стає довільне відділення частини мережі.
- Межі масштабованості - жорстке обмеження по максимальній швидкості транзакцій не може бути знято в рамках децентралізованої природи деяких криптовалют.
- Високі вимоги до апаратної частини - методи, які використовують криптовалюти, що походять від Bitcoin істотно підвищують вимоги до апаратної частини через складну логіки обробки транзакцій.
- Необмежене зростання даних - швидке зростання даних обумовлено збереженням всіх транзакцій.

Мережа ІОТА використовує алгоритм Tangle, який представляє з себе спрямований ациклічний граф:

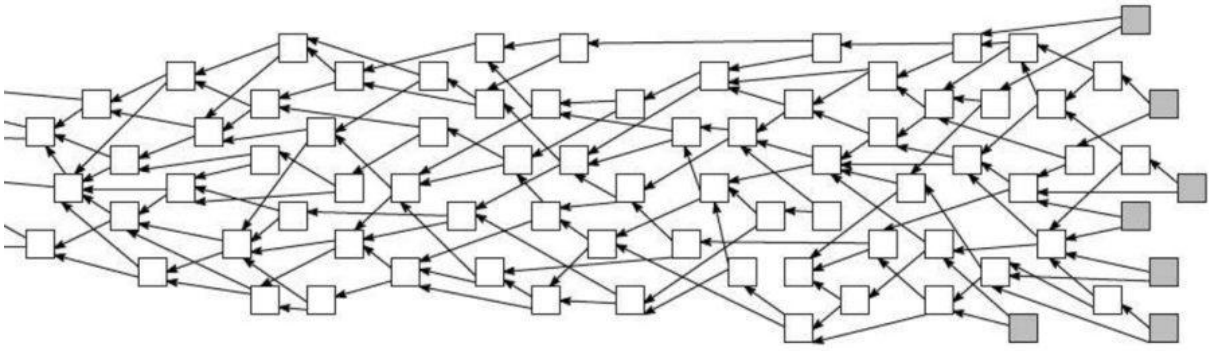


Рисунок 1 – Спрямований ациклічний граф

Мережа DAG складена з транзакцій. Коли з'являється нова транзакція, вона повинна схвалити дві попередні транзакції, ці схвалення представлені спрямованими стрілками (час йде зліва направо). Якщо між двома транзакціями A і B існує шлях довжиною щонайменше в два ділянки, вважається, що A побічно схвалює B. Вузли перевіряють відсутність конфліктів і не схвалюють (прямо чи опосередковано) конфліктуючі транзакції. Ідея полягає в тому, що, у міру того, як транзакція отримує все більше прямих і непрямих схвалень, прийняття її системою збільшується. Іншими словами, при великій кількості схвалень, подвійна витрата стає практично неможливою. Для цього використовується поняття ваги транзакції - це кількість роботи, яку вклав в транзакцію вузол, який її випускає (на практиці це 3 ^ n, де n - ціле число), і кумулятивної ваги, яка представляє собою суму власної ваги транзакції і ваг всіх попередніх транзакцій, що прямо або опосередковано схвалили її.

Щоб провести транзакцію, вузол виконує наступні дії:

- Вузол вибирає дві інші транзакції для затвердження відповідно до алгоритму. Загалом, ці дві транзакції можуть збігатися.
- Вузол перевіряє, чи не конфліктують ці дві транзакції та не схвалюють суперечливі транзакції.
- Щоб вузол видав дійсну транзакцію, він повинен вирішити криптографічне завдання, схоже з завданням в блокчейн Bitcoin.

Важливо зауважити, що IOTA-мережа є асинхронною. Вузли не обов'язково бачать один і той же набір транзакцій. Слід зазначити, що tangle може містити конфліктуючі транзакції. Вузлам не потрібно досягати згоди щодо того, які дійсні транзакції мають право існувати. Однак в разі виникнення конфліктних транзакцій, слід вирішити, які з них не будуть підтверджені. Основне правило, яке використовується вузлами для вибору між двома конфліктуючими транзакціями, полягає в наступному: вузол багато разів виконує алгоритм вибору вершини і бачить, яка з двох транзакцій найімовірніше буде побічно схвалена обраною вершиною. Наприклад, якщо транзакція була обрана 97 разів за 100 прогонів алгоритму вибору вершин, можна вважати, що це підтверджується достовірністю 97%.

Вага транзакції пропорційна обсягу роботи, яку інвестиційний вузол інвестував в неї. У поточній реалізації IOTA вага може приймати тільки значення 3n, де n - натуральне число, яке належить деякому непорожньому інтервалу допустимих значень. Фактично, не обов’язково знати, як вага була отримана на практиці. Важливо тільки, щоб вага кожної транзакції була цілим позитивним числом. Загалом, ідея полягає в тому, що транзакція з великою вагою більш «важлива», ніж транзакція з меншою вагою. Щоб уникнути спаму і інших атак, передбачається, що жодна сутність не може генерувати надлишок транзакцій з «прийнятними» вагами за короткий проміжок часу.

Варто сказати, що інтернет речей цікавий не тільки IOTA, а й великим корпораціям, в числі Samsung, Google і навіть Microsoft. Слід розуміти, що співпраця з деякими з них вже налагоджена. У найближчому майбутньому, адміністрація IOTA планує залучити більше великих компаній до розробки. IOTA є однією з небагатьох долгопланових криптовалют. За прогнозами фахівців кількість з'єднань в світі «Інтернету речей» до 2020 року досягне позначки в 50 млрд, що значно позначиться на потреби користувачів в надійної білінгової мережі з транзакціями без комісій.

ПЕРЕЛІК ПОСИЛАНЬ

1. https://docs.iota.org/
2. https://www.bitbetnews.com/prognoz-kriptovaljut/kriptovaljuta-iota-ee-perspektivy-i-prognoz-2018.html
3. https://distributedlab.com/blog/ru/main-principles-of-iota

УДК 004.056.52

Панасейко Н.М. студентка гр. 121-18-1
Науковий керівник: Сироткіна О.І., к.т.н., доцент кафедри програмного забезпечення комп'ютерних систем
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ПРОБЛЕМИ БЕЗПЕКИ ГРАФІЧНИХ КЛЮЧІВ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ БЛОКУВАННЯ СМАРТФОНІВ

Життя людей сьогодні неможливо уявити без смартфонів, які використовуються не тільки як пристрої зв'язку, але і як сховища особистої інформації: фотографій, повідомлень, заміток, даних про банківські рахунки. Мобільна операційна система(ОС) повинна забезпечувати роботу лише для одного користувача мобільним пристроєм, а також захищати інформацію від сторонніх користувачів. Для цього існують механізми блокування смартфона: паролі, що складаються з літер і цифр, PIN-коди, біометрична автентифікація (за відбитком пальця, сітківки ока, контурами особи, голосу користувача) і графічні ключі.

Патерн або графічний ключ - це задана користувачем послідовність з'єднаних в ламану лінію зображень точок на екрані смартфона. Зображення точок формують поле введення ключа, розмір якого може варіюватися від 3 * 3 до 6 * 6 в залежності від версії ОС і моделі гаджета. Спробувати ввести ключ допускається, як правило, не більше 5 разів. Даний механізм захисту ефективний у разі, якщо телефон не втрачено або просто необхідно приховати дані, що містяться в ньому, від сторонніх очей. Варто зазначити, що такий спосіб блокування допомагає тільки в смартфонах на основі операційної системи (ОС) Android.

Кілька років тому норвезький дослідник Марта Логе зайнялася вивченням графічних ключів. В ході своєї роботи вона проаналізувала 4000 варіантів патернів і з'ясувала, що вони можуть складатися не менше ніж з 4 точок і не більше ніж з 9, а загальна кількість комбінацій становить приблизно 390 тисяч. М. Логе підрахувала, що 44% ключів мають початок у верхній лівій точці і 77% починаються в будь-якому з кутів поля введення. Також вона вирахувала середню кількість точок в ключі - п'ять, а це означає, що зловмиснику, який хоче розблокувати смартфон, доведеться перебрати менше 8000 комбінацій.

Необхідно відзначити, що надійність патерна залежить не тільки від кількості використовуваних точок, а й від послідовності їх сполуки. Якщо привласнити використовуваним в ключі точкам числа, розташувавши їх так само, як вони розташовані на клавіатурі звичайного телефону, вийде, що послідовність 1, 2, 3, 6 куди менш безпечна, ніж 2, 1, 3, 6, яка змінює напрям. Крім цього, М.Логе виявила схожість в уразливості паролів, що складаються з літер, цифр, і графічних ключів. Не менше 10% патернів - букви, і майже завжди з'ясовувалося, що це не просто буква, а перша літера імені самого опитаного, його дружини (чоловіка), дитини і так далі. Якщо зловмисник спробує розблокувати гаджет, знаючи ім'я жертви, то зрозуміло, що йому вдасться зробити це без особливих зусиль.

Група вчених з Ланкастерського університету у Великій Британії змогла вкрасти графічний ключ смартфона, використовуючи лише його мікрофон і динамік. Учені винайшли спеціальну програму SonarSnoop, яка дозволяє користувачеві майже напевно дізнатися графічний пароль від гаджета іншої людини, перебуваючи від неї на відстані. Як заявляють творці, програма здатна аналізувати невеликі зміни положення динаміка, що виникають, коли людина торкається пальцем екрану. Саме за характером цих коливань можна встановити положення пальця на екрані та напрямок його руху. Можливий код виводиться на іншому пристрої. Для демонстрації вчені використовували смартфон Samsung Galaxy S4. Після проведеного випробування програми вона дозволила відкинути 70% варіантів ключа, авжеж цього достатньо, аби дізнатися патерн.

Минулого року британські математики розробили алгоритм, що дозволяє зламати графічне блокування на смартфонах з ОС Android усього за п’ять спроб. Для такого злому

зловмисникові необхідний власний телефон, камера і спеціальна програма, що аналізує в режимі реального часу те, що відбувається перед об’єктивом камери. Вчені пояснили, що зловмиснику не потрібно “підглядати” в екран вашого смартфона, достатньо направити камеру, сидячи збоку або прямо перед власником телефону на відстані в 5-9 метрів і не викликати підозр. Програма розпізнає близько 95% графічних ключів усього з п’яти спроб, причому 87% складних паролів вона вгадує з першого разу, і тільки 40% легких комбінацій не вдається обчислити спочатку. Це дійсно вражає та змушує замислитись над безпекою подібного способу захисту.

Керуючись результатами дослідження, можна запропонувати правила, за допомогою яких графічний ключ стане не тільки зручним, але й ефективним захистом: По-перше, патерн повинен складатися з 8-9 точок. Це обумовлено двома причинами: 1) невелика кількість людей, що використовують довгі ключі; 2) збільшення кількості комбінацій при підборі ключа. По-друге, не варто забувати, що патерни, які складаються з літер, вкрай вразливі до злому. Третя рекомендація: починати «малювати» ключ краще з найменш використовуваних точок, наприклад, із середньої або нижньої точки на правій стороні. І остання рекомендація відноситься до уразливості, виявленої багатьма користувачами смартфонів на практиці. Виявляється, щоб дізнатися графічний ключ досить поглянути на вимкнений екран пристрою під кутом: жирові сліди, залишені пальцями при розблокуванні, проявляють задану послідовність з'єднання точок від початку і до кінця. Отже, після кожного розблокування необхідно протирати екран смартфона серветкою.

Безумовно, блокування за допомогою графічного ключа просте і дуже зручне у використанні, але у цього способу є значні мінуси. Тому патерни все ж не варто використовувати в якості основного механізму захисту смартфону.

ПЕРЕЛІК ПОСИЛАНЬ

1. Розблокування графічного ключа за п’ять спроб: [Електронний ресурс] режим доступу https://pikabu.ru/story/
2. Нефедова М. Нефедова М. Графічні ключі так само передбачувані, як паролі «1234567» и «password» .
3. Бокова О.І., Михайлов Д.М., Фроімсон М.І. Вироблення і аналіз вимог до захищеної мобільної операційної системи.
4. Таненбаум Е., Бос Х. Сучасні операційні системи.

УДК 004.056.5

Сисоєва А.Д. студентка гр. 125м-17-1
Науковий керівник: Войцех С.І., ст. викладач кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАБЕПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ПЛАТІЖНИХ КАРТОК

Оплата за допомогою кредитної картки - це найпопулярніший і найпростіший спосіб оплати товарів і послуг в Інтернеті. Користувач просто вводить номер своєї кредитної картки, ім'я, термін дії картки; торговець підтверджує цю інформацію та ,за погодженням з компанією, що видала кредитну картку, відправляє товар або надає доступ до послуги.

Поява електронної комерції викликала серйозні проблеми щодо забезпечення безпеки даних, тому оператори платежів, виробники електронних карт, а також власники карток продовжують шукати ефективні засоби протидії загрозі шахрайства в Інтернеті. Злочини з кредитними картками здійснюються кількома способами:

- підроблення карток;
- хакерські напади з метою доступу до бази даних клієнтів магазинів;
- створення фальшивих онлайн-магазинів, які використовують процес імітації шляхом відправлення шахрайського електронного листа з проханням поновити реєстраційну інформацію та дані кредитної картки для використання веб-служби (клієнти добровільно подають інформацію про картку);
- отримання віддаленого або фізичного доступу до комп'ютера , на якому тримач картки користувався зручною автоматичною функцією в Інтернеті (запам'ятовування даних, включаючи інформацію про кредитну картку, яка використовується для заповнення веб-форм і зберігає її). У наступний раз, коли потрібно заповнити подібну форму, вона завершує її автоматично, інформація про кредитну картку може бути вкрадена.

Під час придбання товару, дані про оплату передаються між комп'ютером клієнтів та магазином постачальника через Інтернет. Це викликає занепокоєння щодо інтернет-безпеки кредитних карток та крадіжки особистих даних. Більшість інтернет-магазинів захищені, користувач повинен побачити безпечний символ сайту, який відображається веб-браузером, як доказ для подальшого користування сервісом, що надає веб-сайт.

Для ефективного подолання шахрайства сервіс приймання платежів має бути сертифікований міжнародним стандартом безпеки PCI DSS (Payment Card Industry Data Security Standard) [1]. PCI DSS - стандарт безпеки даних індустрії платіжних карт, розроблений Радою зі стандартів безпеки індустрії платіжних карт (Payment Card Industry Security Standards Council, PCI SSC). Будь-яка організація, що планує приймати й обробляти дані банківських карт на своєму сайті, повинна відповідати вимогам PCI DSS. Іншими словами, вимоги - це документація зі списком критеріїв, яким повинен задовольняти сервіс, якщо він управляє такими даними, як номер картки, термін її дії та CVV-код.

PCI DSS описує 12 загальних вимог (які об'єднано в 6 логічно зв'язаних груп) до сервісів безпеки інформаційних систем торгівельних організацій, провайдерів послуг та фінансових інституцій, які оброблюють, зберігають і передають дані тримачів платіжних карт (Табл. 1) [2].

Таблиця1

Загальні вимоги стандарту PCI DSS

Мета	Вимоги
Створення і підтримка безпечної мережі	1. Розробка і забезпечення підтримки конфігурацій міжмережевих екранів для захисту даних тримача карти

	2. Системні паролі та інші параметри безпеки, встановлені виробником, використовувати забороняється.
Захист даних тримача	3. Забезпечення безпеки даних тримачів карт, що зберігають карти
	4. Шифрування даних тримачів карт при передачі їх через відкриті і загальнодоступні мережі
Підтримка програми управління вразливостями	5. Використання і регулярне оновлювання антивірусного програмного забезпечення
	6. Розробка і підтримка безпечних систем і додатків
Впровадження посилених засобів управління доступом	7. Обмеження доступу до даних тримачів карт лише службовою необхідністю
	8. Призначення унікального ідентифікатора кожній особі, що має доступ до комп'ютерної мережі
	9. Обмеження фізичного доступу до даних тримача карти
Регулярний моніторинг і тестування мережевої	10. Відстежування і контролювання будь-якого доступу до мережевих ресурсів і даних тримачів карт
	11. Регулярна перевірка систем і процесів забезпечення безпеки
Підтримка Політики інформаційної безпеки	12. Підтримка Політики, що визначає правила інформаційної безпеки для співробітників і партнерів

Кожна загальна вимога в стандарті деталізована більш конкретними вимогами з описом процедури тестування, що буде виконуватися акредитованим оцінником безпеки (QSA).

В межах PCISSC діють три основні стандарти, які адресовані:

- розробникам та постачальникам пристроїв, які оброблюють номер персональної ідентифікації (PIN) -PCIPTS;
- розробникам і постачальникам платіжних додатків (software developers Payment Application Vendors) -PCIPA-DSS;
- торговцям і процесорам (merchants&processors), які оперують даними тримачів платіжних карт-PCIDSS.

Всі вимоги стандартів охоплюють питання безпеки на рівні мереж, обладнання, додатків, баз даних, фізичних сховищ, документування та управління процесами. Таким чином, якщо компанія збирається приймати й обробляти дані платіжних карт на своєму сайті, їй необхідно пройти сертифікацію на відповідність PCI DSS.

ПЕРЕЛІК ПОСИЛАНЬ

1. Payment Card Industry Security Standards Council– PCI SSC, 2010 / URL: www.pcisecuritystandards.org.
2. Стандарт PCI DSS 3.2

УДК 681.518.54

Добровольський Д. М. студент гр. 125м-17-1
Науковий керівник: Мілінчук Ю.А., асистент кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВРАЗЛИВОСТІ ПЛАТІЖНИХ ТЕРМІНАЛІВ ТА МЕТОДИ ІХ ЗАПОБІГАННЯ

Останнім часом в засобах масової інформації неодноразово піднімаються питання безпеки платежів з використанням мобільних терміналів оплати (mPOS-термінали або ПІН-пади).

Можливо виділити шість основних способів атаки:

Читання трафіку Bluetooth.

Мобільні термінали оплати найчастіше працюють по Bluetooth з мобільним пристроєм (смартфон, планшет). В цьому випадку зловмисники можуть перехопити трафік з'єднання ПІН-пад - смартфон, тобто вкрасти дані власника картки або ПІН-блок. У стандарті PCI PTS чітко прописано, що з'єднання по Bluetooth і / або WiFi має бути шифрованим. Це реалізовано і на ПІН-падах BluePad-50 - будь-яка сесія відбувається в зашифрованому тунелі. Але, подібні з'єднання мають уразливості. Тому, крім шифрування трафіку, всі дані, які смартфон зчитує з ПІН-пада, шифруються різними 3DES ключами на етапі їхнього виконання. При цьому для ПІН-блоку, EMV-даних і службової інформації (дані про ключі і їх заміні) використовується свій ключ шифрування- будь-які дані, що читаються з BluePad-50, завжди зашифровані і розшифровуються тільки на стороні банку! Безпека цих даних визначається надійністю кріптомеханізмов.

Перехоплення ПІН.

Всі дані з ПІН-пада читаються тільки в зашифрованому вигляді - безпека передачі ПІН-коду визначається також надійністю кріптомеханізмів.

Підміна суми транзакції в смартфоні.

Для того, щоб підмінити суму операції в смартфоні, шахраї використовують шкідливе програмне забезпечення на самому смартфоні перед відправкою в банк - смартфон відправляє на сервер прочитаний з ПІН-паду зашифрований ПІН-блок, зашифровані ДДК і EMV-дані (ніяких інших даних більше не передається). EMV-дані включають тег 9F02 (сума транзакції). На основі отриманих даних сервер формує фінансове повідомлення, попередньо розшифровуючи кожен з блоків. Відповідно, можливість отримати суму транзакції і підмінити її визначається тільки надійністю кріптомеханізмов.

Пропозиція використовувати інший інтерфейс.

У мобільних додатках можуть виникати пропозиції використовувати інший, менш захищений інтерфейс, наприклад, магнітну смугу. Запуск шкідливих програм в mPOS для отримання або зміни важливих транзакційних даних.

Мережеві атаки.

З приходом цифрової трансформації банки все більше обростають різними сервісами, відкритими в інтернеті. Відповідно, у різного роду експериментаторів і зловмисників є можливість нанести мережеву атаку на такі сервіси. Сервіси мобільного еквайрингу не є винятком, тому що на відміну від звичайного банківського терміналу мобільний еквайринг працює тільки в інтернеті і не має можливості отримати постійну адресу для побудови тунелю.

Можна виділити кілька методів застереження зловмисникам:

Використання виключно ліцензованого програмного забезпечення в якому буде функція яка забороняє підключення до POS-терміналу.

На даний момент все ще залишається популярним метод злому платіжних систем шляхом відключення від мережі Інтернет POS-терміналів віддалено.

Вчасно повідомляти партнерів про можливі атаки. Вести спостереження загроз, що, в свою чергу, дозволить при необхідності в терміновому порядку заблокувати або вивести дані.

Не застосовувати POS-термінали як частина робочого персонального комп'ютера, а використовувати за призначенням. Також, рекомендується відокремлювати важливі дані і правильно їх розподіляти.

На сьогоднішній день, фахівці кібербезпеки, рекомендують вдосконалювати систему інформаційної безпеки, зокрема дотримуючись загальні правила безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Проект «Рекомендаційний стандарт безпеки банкоматів і платіжних терміналів» - 2013.

2. Шахрайство в платіжній сфері: бізнес-енциклопедія / Лямін Л., Пятіізбянцев Н., Пухов А., Ревенков П., Сачков І., Баулін В., Волков Д., Кузин М., Лобанова І .; під ред. А. Вороніна - М.: Паблішер, 2016. - 430 с.

3. Вечтомов В. Фізичний захист банкоматів // Каталог «Системи цифрового відеореєстрації (DVR)». - №1. - 2013. - С. 46-47.

4. Гріціенко А.А. Основні загрози для банкоматів і платіжних терміналів в сучасних умовах. Презентація - 2014.

5. А. Климов, Н. Рябцев Основні види кримінальних загроз банкоматів і способи протидії цим загрозам // Алгоритм безпеки. - №3. - 2015. - С. 10-13.

6. Образцов С. Способи розкрадань з банкоматів і як з ними боротися // Міжгалузевий тематичний каталог «Безпека та захист - 2017». - 2017. - С. 52-54.

УДК 681.3.06

Хижняк Віталій Володимирович , студент гр. 125м-17-2
Науковий керівник: Войцех Сергій Іванович, ст. викл. кафедри безпеки інформації та телекомунікацій.
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ЗАХИСТ ТЕХНІЧНИХ ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІЇ ВІД ЗАГРОЗ ЧЕРЕЗ МЕРЕЖІ ЕЛЕКТРОЖИВЛЕННЯ

Розглянуто можливі загрози впливу на технічні засоби обробки інформації через мережі електроживлення і захисні можливості різних типів джерел безперебійного живлення. Наведено рекомендації щодо їх використання.

Технічні засоби обробки інформації інформаційно-обчислювальних та інформаційно-комунікаційних систем для своєї роботи потребують джерел та мереж електроживлення. Силовий вплив через ці мережі може призвести до різного рівня порушень в роботі обладнання таких систем.

До основних аварійних ситуацій в мережах електроживлення можна віднести такі, як зникнення, провали, сплески, низький або високий рівень напруги, нелінійні викривлення напруги, перехідні процеси при комутації, електромагнітні та радіочастотні завади, викривлення частоти.

Зокрема, стосовно комп'ютерів це може призвести до втрати інформації в оперативній пам'яті, виникнення помилок, виходу з ладу елементів апаратури, втрати даних, «підвисання» комп'ютерних систем та інших непередбачених наслідків.

Поширеним заходом протидії є використання додаткових пристроїв захисту-джерел безперебійного живлення(ДБЖ).

Джерело безперебійного живлення – це електронний пристрій, призначений для аварійного електроживлення за допомогою акумуляторних батарей при виникненні проблем з електропостачанням. ДБЖ підтримує працездатність навантаження протягом певного часу (часу резервування або часу автономної роботи). Кількість часу, в свою чергу, може бути від декількох хвилин до декількох діб в залежності від потужності навантаження і ємності батарейного комплекту. Джерела безперебійного живлення можуть відрізнятися за принципами роботи, що зумовлює особливості їх використання в технічних засобах обробки інформації [1].

Загалом джерела безперебійного живлення умовно розділені на три основних класи:

1. Резервного типу (Off-line).
2. Лінійно-інтерактивних (Line-interactive).
3. З подвійним перетворенням (On-line).

Джерело безперебійного живлення резервного типу (Off-line) - цей пристрій з автоматичним комутатором в схемі, який при роботі в нормальному режимі забезпечує підключення навантаження безпосередньо до зовнішньої живлячої електромережі, а в автономному - перемикає її на живлення від акумуляторних батарей. Це дозволяє уникнути найбільш поширених проявів нестабільності в мережі-поодиноких імпульсів з великою амплітудою, але дуже малою тривалості(грозові розряди), періодичних відключень електроенергії на підстанціях або добові коливання мережевої напруги внаслідок зміни навантаження на різних фазах[2].

Джерело безперебійного живлення лінійно-інтерактивного типу (Line-interactive) виконане за схемою з комутуючим пристроєм (Offline) і доповнено автоматичним регулятором напруги на основі автотрансформатора зі змінними обмотками (ступінчастим стабілізатором)[3]. Наявність автоматичного регулятора напруги дозволяє корегувати рівень вхідної напруги в широкому діапазоні без переходу на батарейний комплект[4].

Джерело безперебійного живлення з подвійним перетворенням типу (On-line) побудовано на застосуванні принципу подвійного перетворення електричної енергії. Спочатку змінна

напруга з мережі перетворюється в постійну, а потім з постійної напруги формується стабільна по напрузі і формі вихідна змінна напруга[5]. Це позбавляє від впливу негативних змін напруги в мережі електроживлення, до того ж стабілізує величину напруги, корегує коефіцієнт потужності і форму вихідної напруги, що до того ж подовжує термін служби підключених технічних засобів.

Більш детальна інформація про характеристики джерел безперебійного живлення наведена в таблиці 1.

Таблиця 1

Характеристики джерел безперебійного живлення

Характеристики			
Тип ДБЖ	Of-fline	Line-interactive	On-line
Форма вихідної напруги	Трапеціїдальна	Близька до синусоїди	Синусоїда
Стабілізація напруги	Відсутня	Ступенева	Повна
Стабілізація частоти	Відсутня	Відсутня	Є
Фільтрація перешкод	Відсутня	Часткова	Максимальна
Потужність ДБЖ	Малої потужності	Середньої потужності	Великої потужності
Зміна на АКБ	Ступенева	Ступенева	Плавна
Заряд ДБЖ	Малої місткості	Середньої місткості	Великої місткості
Режим Байпас	Відсутній	Відсутній	Є
Додаткове ПО	Відсутнє	Є	Є

Порівняльний аналіз можливостей джерел безперебійного живлення показує, що вони мають різні можливості щодо вирішення проблем, що виникають в мережі електроживлення. Найбільше переваг мають джерела безперебійного живлення з подвійним перетворенням (On-line) і вони можуть бути найкращим вибором при побудові систем захисту від загроз технічним засобам обробки інформації через джерела та мережі електроживлення в інформаційно-комунікаційних системах.

ПЕРЕЛІК ПОСИЛАНЬ

1.Лопухин А.А. Источники бесперебойного питания без секретов. 85с. 2016 р.

2. URL: http://pcm.ru/support/tech/6815

3. URL: https://invertory.ru/category/online-ibp/

УДК 681.518.54

Жук Є.В. студент гр. 125м-17-1
Науковий керівник: Ковалева Ю. В., асистент кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

МАШИННЕ НАВЧАННЯ ДЛЯ НЕТЕХНІЧНИХ ЛЮДЕЙ

Поки ера цифрових інновацій та технологічних проривів продовжується, більшість людей все одно не можуть отримати належне розуміння нейронних мереж, штучного інтелекту та машинного навчання. Ці технології мають такий вплив у нашому житті, що ми не можемо ігнорувати оголошення, повинні отримати базові знання про особливості, переваги та небезпеку машинного розуму.

Реклама, спілкування, пошукові системи, візуальне розпізнавання. В даний час майже кожна послуга яка повинна спілкуватися з людьми в будь-якому випадку, ймовірно, використовує комп'ютерне навчання як основу системи.

Машинне навчання - це область інформатики, яка дає комп'ютерам можливість вчитися, не будучи явно запрограмованою станцією. Потім вони можуть застосовувати те, що вони дізналися з існуючих даних, для прогнозування майбутнього

поведінки, результатів і тенденцій для вирішення проблем. Наприклад, алгоритм може бути навчений по фотографіям, наприклад, собак , зможе розпізнавати собак; той же алгоритм можна також навчити на базі фотографій велосипедів, щоб машина розпізнавала велосипеди без зміни рядка коду.

Існують дві основні категорії: контрольоване навчання і неконтрольоване навчання. Для більшості машин практична цінність навчання сьогодні - це контрольоване навчання. Різниця між контрольованим навчанням і неконтрольованим навчання проста. Для контрольованих уроків ви маєте вхідні змінні (X) і висновок

змінної (Y), і ви використовуєте алгоритм, щоб дізнатися функцію відображення від входу до виходу, щоб отримати Y = F (X).

Неконтрольоване навчання схоже на те, що ви даєте машині тільки деякі дані і говорите «Я не знаю, що відбувається там, просто спробуйте щось зрозуміти. Хай щастить!"

Але що ми повинні дати машині? Як повинні виглядати вихідні дані? Подані вхідні дані припустимо, що це виглядає як податкова книга. Найпростіший приклад - пара стовпців. У першому стовпчику представлені дані в

чиста форма. Це може бути рядок якогось тексту, масив чисел, пікселів, майже всі, що ви можливо, може бути поданий в машину. Другий стовпець повинен відповісти на питання «це тип« A »або тип« B », дані". Аналізуючи цю таблицю, система з машинним навчанням може приймати рішення на основі свого роду нові вхідні дані, які не були представлені в старій таблиці.

Можна взяти більш явний приклад; гіпотетичний алгоритм неавтоматичного навчання розпізнавання осіб в зображеннях намагатиметься визначити, що таке обличчя (круглий шар типу шкіри, з темною областю, де ви очікуєте очей і т.д.). Алгоритм машинного навчання не мав би такого кодованого визначення, але "навчався би за прикладами": ви побачите кілька зображень осіб та осіб без обличчя, і хороший алгоритм в кінцевому випадку навчиться і зможе передбачити, невидимо чи ні невидиме зображення - це обличчя.

Цей конкретний приклад виявлення лиця контролюється, що означає, що ваші приклади повинні бути позначені або явно вказувати, які з них є особами, а які ні.

У неконтрольованому алгоритмі ваші приклади не позначені, тобто ви нічого не говорите. Звичайно, в цьому випадку сам алгоритм не може "придумати", що таке лице але він може спробувати cluster (група однакових або подібних елементів) дані в різні групи, наприклад він може відрізнити, що лице сильно відрізняються від ландшафтів, які сильно відрізняються від коней.

Так як в іншому відповіді згадується (хоча і не так): є "проміжні" форми спостереження, тобто напівконтрольоване та активне навчання. Технічно це контрольовані методи, в яких є певний "розумний" спосіб уникнути великої кількості помічених прикладів. При активному навчанні сам алгоритм вирішує, яка річ підлягає маркуванню (наприклад, він може бути впевнений в пейзажі і собаці, але він може попросити вас підтвердити, чи дійсно горила - зображення обличчя). У напівконтрольованому навчанні є два різних алгоритми, які починаються з помічених прикладів, а потім "повідомляють" один одному, як вони думають про велику кількість немічених даних. З цієї "дискусії" вони навчаються.

Звичайно, виконання проекту машинного навчання в реальному житті набагато складніше, ніж проста формула, великий обсяг даних або порівняння обличчя людей та коней. Необхідно враховувати численні міркування і вирішувати різні завдання що потрібно подолати. Але тепер ми можемо перестати жити в темряві нашого невігластва і зробити перший крок для досягнення нового рівня в технологічному світі.

ПЕРЕЛІК ПОСИЛАНЬ

1. MIT Media Lab [Електронний ресурс] : [Інтернет-портал]. – Can artificial intelligence learn to scare us?– [Massachusetts Institute of Technology]. – Режим доступа: http://news.mit.edu.

УДК 004.7:004.056

Бачурін. О.О. студент гр. 125м-17-1
Науковий керівник: Флоров С.В., к.т.н., доцент кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ОСОБЛИВОСТІ ІНТЕГРАЦІЇ ОФІС 365 З ДИСТАНЦІЙНОЮ СИСТЕМОЮ ОСВІТИ

Особливістю Office 365 та системи дистанційної освіти є те, що вони повинні бути впроваджена на всіх робочих місцях, пов'язаних зі створенням, редагуванням і зберіганням інформації, інакше ефективність від її використання буде мінімальною. Але в процесі впровадження виникає багато проблем, як психологічного так і іншого характеру. Шляхом аналізу було виявлено основні з них:

1) Недостатньо високий статус проекту у ВНЗ. Відсутність зацікавленості керівників підрозділів організації або начальників відділів у впровадженні системи електронного документообігу може призвести до значного подовження строку впровадження або взагалі його провалу.

2) Консерватизм співробітників. Людям, які звикли працювати в звичному для них режимі доведеться зіткнутися з багатьма нововведеннями, навчатися і до того ж не погіршити якість виконання своєї основної роботи. Вирішити цю проблему можна шляхом публікацій туториалов та покрокових інструкцій на веб сайтах ВНЗ, а також морального та матеріального стимулювання у вигляді премій та інших заохочень[1].

Один із двигунів процесу впровадження – зацікавленість користувачів. Відомо, що користувачі, освоївши технологію, згодом вивільняють частину робочого часу. Про це необхідно сказати заздалегідь, щоб дати людям стимул до освоєння системи. [2]

3) Неефективне керування проектом впровадження. Важливим організаційним аспектом є вибір керівника проекту впровадження та формування робочої групи. Це дозволить запобігти затягуванню строків реалізації проекту, уникнути організаційних труднощів завдяки чіткому визначенню обов'язків та послідовно контролювати ефективність досягнення цілей проекту.

4) Треба провести попередню перебудову бізнес-процесів освіти до переходу до інтеграції eOffice 365 з системою дистанційної освіти, інакше проблеми, які існували у паперовому документообігу лише посиляться[3].

5) Проблема адаптації студентів. Навчання студентів – це процес двосторонній. З одного боку, вони вчаться працювати в системі, з іншого – їх зауваження та побажання дають можливість команді яка впроваджує систему врахувати всі нюанси робочих процесів і адаптувати систему до специфіки організації. [6]

7) Трансформація документів з паперової форми в електронну. Для переводу паперових документів в електронну форму повинні використовуватися сканери. Більшість систем документообігу або поставляються з модулями для сканування документів, або передбачають інтеграцію з однією з існуючих систем вводу зображень. Зазвичай, ніякі спеціалізовані системи не потрібні, достатньо будь-якої програми сканування або розпізнавання. При великих обсягах необхідно розглянути необхідність використання професійних систем, призначених для отримання зображення документів. Ці системи дозволяють здійснювати масове введення документів з організацією окремих робочих місць для різних типів робіт, з виділеними серверами для обробки, конвертації і розпізнавання зображень. Вбудовані в них алгоритми дозволяють одержувати зображення високої якості з максимальною швидкістю.

8) Помилкове або неповне визначення задач, які повинні виконувати Office 365 та система дистанційної освіти на етапі розробки технічного завдання, що призводить до необхідності модифікувати прийняте рішення на етапі впровадження.

9) Відсутність регламентів, послідовності дій по роботі з документами. Підготовка нормативних правил, інструкцій з процесів електронного документообігу повинна вестися паралельно з дослідною експлуатацією.

10) Складність інтеграції з вже існуючими системами. На підприємстві можуть існувати інформаційні системи, які використовуються в роботі з документообігом. У такій ситуації потрібна інтеграція з вже існуючим набором комп'ютерних програм.

11) Неможливість виявлення всіх недоліків у функціонуванні на етапі пілотного проекту. Навіть за умови добре організованого та налагодженого пілотного проекту неможливо виявити всі проблеми, які можуть проявитися згодом під час повномасштабного впровадження. Наприклад, навантаження на сервери обробки документів та сервери системи дистанційної освіти може збільшитися суттєвіше ніж очікувалося, що викличе збої в роботі обладнання і паралізує роботу всієї організації. [3,4,9]

ВИСНОВОК

Щороку з'являються нові версії програмного забезпечення, що розширюють вже існуючий функціонал Office 365 що дозволяє використовувати системи дистанційної освіти для управління освітніми процесами.

Передбачення появи зазначених вище проблем ще на етапі розробки технічного завдання на впровадження подібних систем дозволить зменшити їх вплив або навіть уникнути їх появи шляхом якісної організації процесу розгортання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Get the most from Office with Office 365 [Електронний ресурс]. – Режим доступу: https://products.office.com/en-us/compare-all-microsoft-office-products (дата звернення 05.04.2017), вільний.
2. Матвієнко О., Цивін М. Основи організації електронного документообігу. Навчальний посібник. – К.: ЦУЛ, 2008.-112с.
3. Мировой рынок систем електронного документооборота (Електрон.ресурс) /Спосіб доступу: URL: http: http://www.citforum.ru/ – Загол. з екрана.
4. Внедрение систем электронного документооборота:проблемы и решения (Електрон.ресурс) /Спосіб доступу: URL: http: http://www. iteam.ru/ – Загол. з екрана.
5. Средства интеграции Office 365 [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/ru-RU/download/confirmation.aspx?id=26552 (дата звернення 05.04.2016), вільний
6. Необходимость внедрения систем електронного документооборота (Електрон.ресурс) /Спосіб доступу: URL: http://chief.nnov.ru – Загол. з екрана.
7. Лазарєв Г.П., Кльоцкін С.М., Хорошко В.О. Шляхи вирішення проблем інформаційної безпеки в Україні // Захист інформації. – 2008. – № 2. – С. 4-9.
8. Тунда В. А. Руководство по работе в Moodle 3.1. Для начинающих. – Томск, 2015.

УДК 004.7:004.056

Ткачик О.С. студент гр. 125м-17-2
Науковий керівник: Флоров С.В., к.т.н., доцент кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВІДДАЛЕНЕ УПРАВЛІННЯ ІНФОРМАЦІЄЮ У КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЯХ

Інформація та підтримують її інформаційні системи є цінними виробничими ресурсами організації. Їх доступність, цілісність та конфіденційність можуть мати особливе значення для забезпечення працездатності підприємства. З розвитком сучасних засобів мобільного зв'язку і збільшенням зони покриття операторами, мобільні пристрої і мобільні користувачі стають невід'ємною частиною корпоративних мереж Організації стикаються зі зростаючою загрозою порушення режиму безпеки, що виходить від цілого ряду джерел. Для кожної конкретної інформаційної системи політика безпеки повинна бути індивідуальною. Вона залежить від технології і способів обробки інформації, використовуваних програмних і технічних засобів, архітектури локальної мережі, структури організації та виду її діяльності, а також інших факторів. Інформаційних систем і мереж можуть загрожувати такі небезпеки, як комп'ютерне шахрайство, шпигунство, саботаж, вандалізм, а також інші джерела відмов і аварій..

Згідно [1], найбільш актуальними для корпоративних интрасетей використовують мобільні пристрої, є наступні фактори:

- Різке збільшення віддалених мобільних користувачів корпоративних интрасетей, що використовують технології Wi-Fi, GPRS, 3G, 4G.
- У користувачів корпоративних інформаційних систем з'явилися мобільні пристрої нового покоління (iPhone, iPad, Android, Windows 10), що істотно підвищило ймовірність несанкціонованого доступу в интрасеть підприємства за рахунок втрати контролю користувача над мобільним пристроєм.
- Поява технологій і обладнання, що дозволяють перехопити і дешифрувати трафік від віддаленого користувача в интрасеть підприємства.
- У зв'язку з цим виникла необхідність в захисті трафіку від мобільних пристроїв до локальної мережі підприємства.
- Виникла необхідність в централізованому управлінні доступом до web-сервісів интрамережі підприємства при виникненні підозри про зміну його власника або компрометації пароля шифрування. Увімкнувши служби шифрування Office 365, з'являється можливість шифрувати переписку з сторонніми користувачами. Адміністратори можуть задавати алгоритми шифрування і підписування документів.
- Надання доступу користувачам. Послуги Office 365 захищаються на наступних рівнях: ЦОД, мережевий, логічний, рівень зберігання та передачі. Office 365 інтегрується з локальної службою каталогів Active Directory і іншими системами зберігання і ідентифікації каталогів.

Одним з ефективних варіантів розв'язання проблеми є:

1. Розгортання інфраструктури відкритого ключа в інтрамережі підприємства.
2. Отримання та встановлення сертифікатів на мобільні пристрої користувачів корпоративної інтрамережі.
3. Забезпечення віддаленого управління інформацією в разі втрати контролю користувача над мобільним пристроєм.
4. Розробка програмного забезпечення, що дозволяє встановлювати сертифікати на мобільні пристрої користувачів.
5. Розгортання в домені підприємства служби Mobile Administration Web tool, що дозволяє блокувати інформацію на на мобільних пристроях при виникненні підозри у втраті контролю.

В корпоративних мережах під керуванням Windows управління функцією дистанційного стирання пам'яті, виконуваної пакетом Messaging and Security Feature Pack, здійснюється за допомогою інструменту веб-адміністрування ActiveSync Mobile Administrative Web Tool. Цей інструмент дозволяє управляти процедурою дистанційного стирання пам'яті загублених, вкрадених або іншим чином потрапили в чужі руки мобільних пристроїв, підключених до серверів по бездротових з'єднань.

При гібридному способи розгортання корпоративної мережі необхідно використовувати хмарний сервіс Mobile Device Management який дозволяє взяти під контроль мобільні пристрої співробітників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Моримото, Рэнд, Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Microsoft Windows Server 2016. Полное руководство. : Пер. с англ. — М. ,2017. — 1456 2.
2. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Утверждено приказом Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины от 28 апреля 1999 г. № 22. // Официальный сайт Службы безопасности Украины. Способ доступа: URL: http: // www.dstszi.gov.ua/.
3. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» (Электрон. ресурс)/Способ доступа: URL: http://www.dstszi.gov.ua/dstszi
4. ISO/IEC 27005:2005 «Інформаційні технологій. Методи захисту. Система управління інформаційною безпекою. Вимоги» (Электрон. Ресурс)/Способ доступа: URL: http://www.dstszi.gov.ua/dstszi/control
5. MDM Migration Analysis Tool/(Електрон. ресурс)/Способ доступа: URL: https://www.microsoft.com/enus/download/details.aspx?id=7887&fa43d42b-25b5-4a42-fe9b-1634f450f5ee=True

УДК 62-768:537.531

Васильєв Д.Г., студент гр. 125м-17-2
Науковий керівник: Войцех С.І., старший викладач кафедри безпеки інформації та комунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

РАДІОНЕПРОНИКНІ ТКАНИНИ, ЯК ПЕРСПЕКТИВНИЙ МАТЕРІАЛ ДЛЯ ЕКРАНУВАННЯ

Інформаційні технології постійно вдосконалюються у напрямку їх автоматизації і способів захисту інформації [1].

Використання технічних засобів обробки інформації (ТЗПІ) створює проблему виникнення технічного каналу витоку інформації (ТКВІ) з обмеженим доступом через побічні електромагнітні випромінювання. Одним з найбільш ефективних засобів захисту від витоку даних цим каналом є екранування. На сьогодні, широко використовуються екрани з металевих листів, пластин, сіток та ін.. Але у зв'язку з новітніми досягненнями в області вивчення та аналізу широкосмугових електромагнітних полів, підвищенням вимог до захищеності важливої інформації, а також можливими конструктивними обмеженнями, актуальним і сучасним напрямом є використання радіонепроникних тканин в якості екрану [2].

Технічним каналом витоку інформації називається сукупність джерела конфіденційної інформації, середовища поширення і засобу технічної розвідки [3].

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення та способів перехоплення, технічні канали витоку інформації, що обробляється ТЗПІ, можна розділити на електромагнітні, електричні і параметричний.

Електромагнітні випромінювання елементів ТЗПІ утворюються внаслідок того, що в ТЗПІ носієм інформації є електричний струм, параметри якого можуть змінюватися по закону зміни інформаційного сигналу. При проходженні електричного струму по струмопровідним елементам ТЗПІ, навколо них виникає електричне та магнітне поле. Елементи ТЗПІ можна розглядати як випромінювачі електромагнітного поля, модульованого інформаційним сигналом [4].

Для боротьби з побічними електромагнітними випромінюваннями, з-поміж інших засобів, застосовуються спеціальні екрануючі конструкції і матеріали.

Зазвичай в якості матеріалів для ефективного екранування використовуються металеві листи і сітки. Сталеві листи товщиною 2-3 мм, зварені герметичним швом, забезпечують найбільший екрануючий ефект (до 100 і більше дБ) [5].

Останнім часом все ширше застосовуються фольгові і металізовані матеріали, струмопровідні фарби і клеї, радіопоглинаючі будівельні матеріали.

Однак металеві листи мають високу ціну, а виготовлення з них екранів і їх експлуатація вимагають великих витрат. Корозія, що з'являється під час монтажу та напруженість зварювальних швів знижують надійність і довговічність екранів, а необхідність їх періодичної перевірки та усунення дефектів підвищують експлуатаційні витрати [5]. Тому зараз невпинно йдуть пошуки та розробка нових, більш зручних та не менш ефективних матеріалів, які надалі можна бути використовувати в якості альтернативи до класичних матеріалів та конструкцій з них. Одним з таких перспективних матеріалів є радіонепроникні тканини.

В останні роки використання такого типу тканин для виготовлення екранів стає все більш поширеним. Такі екрани володіють досить вагомими перевагами у порівнянні зі звичайними металевими пластинами. Серед них: невисока вага, гнучкість, легкість виготовлення і монтажу та ін.. За кордоном на даний момент розроблено значну кількість тканин, які за своїми екрануючими властивостями не поступаються екранам з металічних пластин. Так, наприклад, коефіцієнт екранування тканини зразка «Aaronia Shield» сягає 50 дБ [6]. Вітчизняні розробки у цій галузі просуваються значно повільніше. Зразки, що наявні на

нашому ринку, поступаються зарубіжним аналогам, а використання останніх ускладнене тим, що їх середня ціна доволі висока [7].

Тому актуальною є задача покращення екрануючих властивостей радіонепрозорих тканин на вітчизняному рівні з попереднім опрацюванням зарубіжних результатів дослідження. Адже на відміну від звичайної металевої пластини, тканини на основі металізованих ниток мають більше параметрів, від яких залежить ефективність екранування. До таких параметрів належать спосіб виготовлення (ткані, трикотажні, неткані), розташування волокон, розмір пор та кількість металу у тканинному екрані та ін. [8]. Також перспективним є дослідження ефективності екранування тканин у комбінації з іншими типами екранів.

Слід зазначити, що вплив на ефективність екранування таких явищ як поглинання та відбиття, безпосередньо залежить від технології виготовлення радіонепроникних тканин. На сьогодні відсутній єдиний стандарт оцінки ефективності екранування таких матеріалів, що породжує відмінності у результатах проведених лабораторних досліджень [9].

Стрімкий розвиток технологій обробки інформації спонукає до пошуку нових та покращення вже існуючих способів захисту інформації. Радіонепроникні тканини мають низку переваг з-поміж інших матеріалів і гарний потенціал розвитку. Тому дослідження їх властивостей та покращення характеристик вже існуючих зразків залишається актуальною темою. При проведенні таких досліджень обов'язково потрібно звертати увагу на вплив характерних для тканин додаткових параметрів. Наявність цих параметрів обумовлена властивостями цих матеріалів і особливостями їх виготовлення та може безпосередньо впливати на ефективність екранування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др..; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
2. Самоквасова Ю.Н. Методика выбора конструкционных материалов для задач экранирования электронных средств / Самоквасова Ю.Н. Ромащенко М.А.
3. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97
4. Хорев А.А. Техническая Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. – 436 с.
5. Средства экранирования электромагнитных полей [Електронний ресурс]. – Режим доступу:http://www.delphiplus.org/inzhenerno-tekhnicheskaya-zashchita-informatsii /sredstva-ekranirovaniya-elektromagnitnykh-polei.html
6. Hoch transparenter 50dB Abschirmstoff for HF und elektrisches Feld Aaronia Shield [Електронний ресурс]: Aaronia AG. — Режим доступу: http://www.aaronia.de/produkte/abschirmungen/Aaronia-Shield-50dB/
7. Дослідження характеристик вітчизняних радіонепрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю.Є. Яремчук, В.С. Катаєв, М.Ю. Гижко, П.В. Павловський // Реєстрація, зберігання і обробка даних. — 2016. — Т. 18, № 1. — С. 42-51.
8. Hulle A, Powar A. Textiles as EMI Shields. // J Textile Sci Eng, 2018, 8: 347
9. WIĘCKOWSKI, Tadeusz W.; JANUKIEWICZ, Jaroslaw M. Methods for evaluating the shielding effectiveness of textiles. *Fibres & Textiles in Eastern Europe*, 2006, 5 (59): 18—22

УДК 004.7.056.5

Воловатов А.В. студент гр. 125м-17-1
Науковий керівник: Кручінін О.В. ст. викладач кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ У ДЕРЖАВНИХ ЗАКЛАДАХ

Виконано аналіз системи електронного документообігу на наявність вразливостей. Розглянули детально особливості електронного цифрового підпису на документах формата *docx, *xls , а також файлів мультимедії, як одного із форматів електронного документообігу та їх вразливості.

В даний час всі державні служби переходять від паперової форми документообігу до електронного документообігу. На даний момент в Україні , розроблена законодавча база яка сприяє введення в дію електронного документообігу. Верховна Рада ухвалила для цього відповідні закони: «Про електроні документи та електронний документообіг», «Про електронний цифровий підпис », «Про обов'язковий примірник документів» , «Про захист інформації в інформаційно-телекомунікаційних системах» , «Про основні засади забезпечення кібербезпеки України » тощо.

Згідно с законом України «Про електроні документи та електронний документообіг »:

- *електронний документ* – це документ, інформація у якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, зокрема, електронний цифровий підпис.
- *електронний документообіг* (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. [1]

На початку 2017 року був прийнятий закон України «Про основні засади забезпечення кібербезпеки України», в якому вказано , що один із об'єктів кіберзахисту є комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сфері електронний документообіг. [2]

Варто зазначити, електронний документ має таку ж юридичну силу як і паперовий. Щоб підтвердити цілісність електронного документа, накладається електронний цифровий підпис, який прирівнюється до власноручного підпису або печатки.

- *Електронний цифровий підпис*-вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача

Перевагами використання електронного документообігу є :

- перехід до більш зручного, швидкого і економного без паперового юридично значимого документообігу;
- удосконалення процедури підготовки, подачі / доставки, обліку та зберігання документів, їх аутентифікація, цілісність, конфіденційність і неспростовність;
- криптографічний захист інформації (електронних документів) при передачі по відкритих каналах;
- мінімізація фінансових ризиків за рахунок підвищення конфіденційності інформаційного обміну документами;
- економія ресурсів за рахунок використання оперативного електронного архіву;
- можливість швидкого пошуку і перегляду електронних документів, а також визначення їх юридичної сили по ЕЦП;

- значне скорочення процедури підписання договорів, оформлення та подання податкової та фінансової звітності;
- швидкий і надійний обмін електронними документами з партнерами, контрагентами незалежно від віддаленості адресата.

В електронному документообігу можуть використовуватись різноманітні формати документів, наприклад:

- документи з ропширенням *docx,*xls,* pdf;
- документи важко зміні *rtf,*html;
- та файли мультимедійні *mpeg, *avi.

Для того щоб , мати змогу підписувати електроні документи з допомогою ЕЦП, користувачу необхідно звернутися до акредитованих центрів сертифікації ключів для отримання сертифікату. Сертифікат містить: закритий та відкритий ключ та ідентифікаційний номер замовника(сертифікат ЕЦП). Ці послуги можливо замовити в одному із 13 акредитованих центрів сертифікації ключів , наприклад:

- Акредитований центр сертифікації ключів ПАТ КБ «ПРИВАТБАНК»;
- Акредитований центр сертифікації ключів Міністерства внутрішніх справ України;
- Акредитований центр сертифікації ключів Інформаційно-довідкового департаменту ДФС.

Центри сертифікації ключів повинні вести обслуговування електронного цифрового підпису від початку її дії до кінця дії сертифіката . До їх обов'язків входить – надання консультації та вирішення проблема пов'язанні з електронним цифровим підписом та ключами , також технічне обслуговування на час дії сертифіката та блокування або повне знищення ключів та електронно цифрового підпису якщо надійшло офіційний запит. Але у зв'язку з постановою КМУ від 19 вересня 2018 року «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності» , можливі зміни стосовно вимог до акредитованих центрів сертифікації України.

Автоматизація електронного документообігу відбувається , за рахунок спеціалізованих систем ,наприклад:

- «Система електронного документообігу АСКОД», «Діловодство», «Кодекс: Документообіг», використовується в більшості наших державних закладах (суд, податкова, тощо);
- «Lotus Notes», «OPTiMA-WorkFlow», використовується в банках, на підприємствах різного виду діяльності .

Кожна з цих систем має свої призначення та деякі з них мають діючий експертний висновок та рекомендовані до використання Держспецзв'язку України, наприклад:

- *Система електронного документообігу* **АСКОД** - В обсязі функцій, зазначених в документі «Часткове технічне завдання на розробку захищеного від НСД компонента «Система електроного документообігу АСКОД. Програмне забезпечення АСКОД Корпоративний», сукупність яких визначається функціоналним профілем захищеності: КА-2, КО-1, ЦА-1, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НИ-3, НК-1, НО-3, НЦ-1, НТ-2, НА-2, з рівнем гарантій Г-2 коректності їх реалізації згідно з НД ТЗІ 2.5-004-99. [3]
- Система «**Діловодство**» - призначена для автоматизації управлінської діяльності у вітчизняних міністерствах і відомствах, територіальних органах влади, на підприємствах різних сфер діяльності.
- Система «**Кодекс: Документообіг**» - це комплекс взаємозалежних систем діловодства, банків документів і корпоративних сервісів, що забезпечують автоматизоване розв' язання задач діловодства і документообігу в органах державної влади й інших організацій.
- Система «Lotus Notes» - забезпечує розроблення і розміщення прикладних програм групового забезпечення, дозволяє користувачам одержувати, відслідковувати, спільно використовувати і створювати інформацію для обробки документів.

Технології, які використовуються в казаних системах, враховуються при побудові систем електронного документообігу. Але система електронного документообігу не може існувати окремо, вона є частиною інформаційної системеми. В зв'язку з цим, механізми захисту систем документообігу повинні взаємодіяти з механізмами інших елементів комплексу засобів захисту.

В результаті проведеного аналізу системи електронного документообігу, можливо зробити такі висновки:

1. Є актуальними питання:
- Яким чином можливо накладання ЕЦП на мультимедійні файли.
- Які формати крім *mpeg , * avi можливо використовувати в системі електронного документообігу.
- Чи є вірогідність можливості зміни контенту медійних файлів , без зміни значення ЕЦП.

2. Необхідно дослідити взаємний вплив механізмів захисту систем електронного документообігу з механізмами інших елементів комплексу засобів захисту

ПЕРЕЛІК ПОСИЛАНЬ

1. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. (http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288071&cat_id=44795)

2. Закон України «Про основні засади забезпечення кібербезпеки України». (http://zakon.rada.gov.ua/laws/show/2163-19)

3. Закон України «Про електронний документ та електронний документообіг» (http://zakon.rada.gov.ua/laws/show/851-15)

УДК 004

Горошко Є.О. студент гр. 125м-17-1
Науковий керівник: Кручінін О.В. старший викладач кафедри безпеки інформаціїї та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ОСНОВНІ ВРАЗЛИВОСТІ ТА ЗАСОБИ КОМПРОМЕТАЦІЇ IOT-ДЕВАЙСІВ 2018 РОКУ

В роботі проведений аналітичний огляд тенденцій розвитку засобів компрометації IoT-девайсів. Також розглянуті основні загрози, вразливості через які вони реалізуються та особливості дії кожної з загроз.

ВСТУП

Нинішній етап розвитку технологій засобів комунікації між пристроями в інформаційних системах сприяв створенню нового способу взаємодії між пристроями в інтернеті. Ця взаємодія не потребує участі людини. Такий концепт взаємозв'язку речей має назву «інтернет речей» (IoT). Але цей вид взаємодії приніс не лише зручність, а й нові загрози.

Фахівці компанії Check Point оприлюднили звіт Global Threat Impact Index за липень 2018 року. Дослідники відзначають, що з травня 2018 роки кількість атак, пов'язаних з поширенням малварі для IoT (Mirai, IoTroop / Reaper і VPNFilter), збільшилася більш ніж в два рази. В рейтинг десяти найбільш часто експлуатованих вразливостей увійшли відразу три проблеми IoT-пристроїв: віддалене виконання коду MVPower DVR маршрутизатора; віддалене виконання команд маршрутизатора D-Link DSL-2750B; обхід аутентифікації маршрутизатора DANAN GPON A. В липні 2018 року 45% організацій в усьому світі піддалися атакам на ці уразливості. «Відомі вразливості надають кіберзлочинцям просту і відносно безперешкодну точку входу в корпоративні мережі, що дозволяє їм виконувати широкий спектр атак. Уразливості пристроїв інтернету речей часто є "шляхом найменшого опору", оскільки, як тільки один пристрій скомпрометовано, через нього можна проникнути в інші підключені до нього пристрої. Таким чином, для забезпечення безпеки мереж організаціям вкрай важливо встановлювати патчі для відомих вразливостей, як тільки вони стають доступні » – коментує Василь Дягілєв, глава представництва Check Point Software Technologies в СНД.

Тож, як показує статистика дослідження – одна з найпоширеніших загроз використання компрометованих пристроїв «інтернету речей» є релізація на їх основі бот-мереж. Такі бот-мережі найбільш розповсджено використовують для проведення DDoS атак.

ОГЛЯД АКТУАЛЬНИХ BOTNET НА ОСНОВІ IOT-ПРИСТРОЇВ

Новітня і найбільш комплексна загроза в світі IoT - це ботнет VPNFilter. Вже незабаром після першого виявлення, VPNFilter заразив півмільйона роутерів Linksys, MikroTik, NETGEAR і TP-Link, а також NAS виробництва QNAP в 54 країнах світу. Оператори VPNFilter здатні перехоплювати трафік і облікові дані закритих мереж і систем; можуть виявляти промислове SCADA-обладнання та заражати його спеціалізованим малваром; можуть використовувати заражені пристрої як звичайний ботнет, приховуючи за ним різні атаки; і, нарешті, можуть просто вивести з ладу сотні тисяч пристроїв.

Також важливим етапов в розвиненні IoT-ботнетів є Hide 'N Seek (HNS). Він був помічений фахівцями ІБ в січні 2018 року. Тоді аналітики компанії Bitdefender попереджали, що нова загроза, атакуюча IoT-девайси, скомпрометувала більше 24 000 пристроїв і продовжує розростатися. Дослідники виявили, що нові версії малварі стали першими з усіх відомих IoT-загроз, які навчилися «переживати» перезавантаження заражених пристроїв і продовжують працювати навіть після цього. З оновленого на початку липня звіту про діяльність HNS з'ясувалося, що ботнет вже

не можна вважати чистою IoT-загрозою, так як він навчився атакувати вразливі БД, крім роутерів і DVR. Так, малвар становить загрозу для OrientDB і CouchDB, пристроїв AVTECH, Cisco Linksys, TP-Link і Netgear. Компанія HomeMatic, постачальник різних рішень для «розумних» будинків вказує на те, що HNS навчився атакувати центральний елемент платформи автоматизації, який використовується для контролю, моніторингу та налаштування всіх пристроїв HomeMatic. «Hide 'N Seek оперативно додає нові експлоїти і атакує все більше платформ і пристроїв, щоб збільшити свою область поширення. Поповнення арсеналу свіжими PoC-експлойтів збільшує шанси того, що HNS першим заразить ці пристрої», – пишуть дослідники.

Що стосується Reaper, цей вірус має певну схожість з Mirai, але насправді це повністю новий і набагато більш складний шкідник, який стрімко поширюється по світу. Однак новий вірус використовує відомі уразливості девайсів. У базі Reaper міститься інформація про пристрої: D-Link, Netgear, Linksys, AVTech, Vacron, JAWS і GoAhead. Коментуючи ситуацію, Надир Ізраель (Nadir Izrael), співзасновник компанії Armis, що забезпечує безпеку інтернету речей, вказав на проблему оновлень. Він зазначив, що більшість підключених девайсів оновити не так просто. На деяких стоїть стандартний пароль, який власник може не знати. А частина взагалі не підтримує оновлення. Фахівці проаналізували код Reaper і виявили, що вірус здатний проводити DDoS-атаки, але їх поки не було. Ймовірно, автор вірусу чекає, поки той поширюється по світу. Заражені пристрої автоматично розсилають вірус на інші підключені гаджети - за даними Check Point Research, цим «займається» приблизно 60% корпоративних мереж, що є частиною глобальної мережі ThreatCloud.

ВИСНОВОК

Не дивлячись на те, що bot-мережі є вже давно відомим інструментом правопорушників у кіберпросторі – зараз існує дуже мало засобів та заходів протидії до цього виду загроз. Це пояснюється стрімким розвитком технологій швидкої передачі даних та збільшенням кількості самих пристроїв, як самостійних одиниць в мережі. Це підводить нас до висновку, що ми маємо забазпечувати безпеку інформаційних систем навіть у дуже невизначених умовах. Необхідно адаптувати існуючі засоби профілактики, боротьби та виявлення бот-мереж до постійно-змінного інтернету речей та пристроїв, що належать до нього.

ПЕРЕЛІК ПОСИЛАНЬ

К. О. Кіфорчук, М. В. Грайворонський – «Оцінка вразливості пристроїв «інтернету речей»»

https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/

https://xakep.ru/2018/07/25/hns-attacks-homematic/

https://www.fortinet.com/blog/threat-research/hide--n-seek--from-home-routers-to-smart-home-insecurities.html?utm_source=security_week

https://blog.talosintelligence.com/2018/05/VPNFilter.html

УДК 004.056

Гриб Михайло Олексійович, студент гр. 125м-17-1
Науковий керівник: Кручінін О.В. старший викладач кафедри безпеки інформаціїї та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВПЛИВ ВИБРУ CMS НА БЕЗПЕКУ ВЕБ-ДОДАТКІВ

В роботі висвітлені основні вразливості веб-додатків та виконано аналітичний огляд сучасних CMS. Проаналізовано вплив надійності CMS на безпеку веб-додатків. Сформульовані загальні рекомендації з захисту веб-додатків.

Ключові слова: Веб-додаток, CMS, web.

ВСТУП

З кожним роком сфера застосування веб-технологій розширюється. Більшість компаній використовує веб-додатки у своїй діяльності: для роботи з клієнтами, забезпечення внутрішніх бізнес-процесів. Вразливості веб-додатків надають зловмисникам широкий простір для дій. Помилки проектування і адміністрування дозволяють атакуючим отримувати важливу інформацію, а також порушувати функціонування веб-додатка, здійснювати атаки на відмову в обслуговуванні, проводити атаки на користувачів, проникати у внутрішню мережу компанії і отримувати доступ до критично значущих ресурсів.

Вразливість системи (system vulnerability) – нездатність системи протистояти реалізації певної загрози або сукупності загроз[1].

Вразливість може бути результатом помилок програмування, недоліків, допущених при проектуванні, експлуатації, а також ненадійних паролів, вірусів[2].

Вразливості можна класифікувати по етапах життєвого циклу програмного забезпечення, на яких вони з'являються:

• вразливості етапу проектування;
• вразливості етапу реалізації;
• вразливості етапу експлуатації.

У наш час для найбільш зручного та простого управління вмістом (контентом) часто використовують системи управління вмістом сайту – Content Management System (CMS). Такі системи допомагають веб-майстрам спростити програмування, дизайн, підтримку сайту і навіть поручати роботу з сайтом людям, які не знайомі з програмуванням та архітектурою web.

Система керування вмістом (англ. Content Management System, CMS) — програмне забезпечення для організації веб-сайтів чи інших інформаційних ресурсів в Інтернеті чи окремих комп'ютерних мережах. Код CMS виконується великою частиною на сервері і забезпечує публікацію матеріалів на сайті, а також зручне управління цими публікаціями із веб-інтерфейсу

Основні функції системи керування вмістом [3]:

- надання інструментів для створення вмісту, організація спільної роботи над вмістом;
- управління вмістом: зберігання, контроль версій, дотримання режиму доступу, управління потоком документів і т. п.;
- публікація вмісту;
- подання інформації у виді, зручному для навігації, пошуку.

ОГЛЯД НАЙПОШИРЕНІШИХ CMS ТА ЇХ ВРАЗИЛОВОСТІ

В залежності від способу розповсюдження розрізняють CMS двох видів: комерційні та вільно поширювані[3].

Безкоштовні CMS поширюються у вільному доступі. Більшість поширених безкоштовних CMS надають безкоштовну підтримку за допомогою спільноти на власних форумах або ж спеціалізованих email-розсилок (наприклад Joomla, WordPress та Drupal).

Платні CMS поділяються на два типи:

- системи із закритим кодом (вихідний код закодований (криптованний) і не допускає будь-яких змін);
- системи з відкритим кодом (для внесення зміни будь-якої з функціональних можливостей вихідний код відкритий).

Згідно з даними сервіса SiteSecure і проекту Ruward[4], які провели комплексне дослідження безпеки сайтів, створених на різних CMS-системах в жовтні 2013 – січні 2014 року, сайти, які користуються безкоштовними CMS, в середньому у 4 рази частіше піддаються зараженням і попадають у чорні списки, ніж сайти на комерційних CMS.

Відповідно даним джерела, частка заражених сайтів виглядає таким чином:

1. DataLife (платна) – 29%;
2. InstantCMS (безкоштовна) – 19%;
3. Joomla (безкоштовна) – 14%;
4. MaxSite CMS (безкоштовна) – 12%;
5. WordPress (безкоштовна) – 5%;
6. 1C-Bitrix (платна) – 3% та ін.

Згідно з проміжних даних сервісу IT рейтинг України[5] за 2018 рік найпопулярнішими CMS в Україні є:

1. WordPress (безкоштовна);
2. OpenCart (безкоштовна);
3. Joomla (безкоштовна);
4. MODX (безкоштовна);
5. 1C-Bitrix (платна).

Проблема безкоштовних CMS в тому, що при розширенні функціональності сайту, використовуються спеціальні плагіни, враховуючи їх недостатній рівень безпеки можливі утворення вразливостей. Крім того, системи постійно удосконалюються, і їх необхідно своєчасно оновлювати. Тому зломи сайтів на безкоштовних CMS найчастіше відбуваються через ігнорування нових версій систем і після установлення плагінів сумнівного походження.

Платні CMS при дослідженні кількості злому сайтів на різних CMS виявляються більш безпечними, при використанні платних систем складніше пропустити важливі оновлення а значить, підвищуються шанси підвищити базовий рівень безпеки.

РЕКОМЕНДАЦІЇ ЗАХИСТУ ВЕБ-ДОДАТКІВ

Згідно з даних Яндекса [6] щоб знизити вірогідність компрометації CMS потрібно дотримуватися таких правил:

1. Регулярно оновлювати CMS.
2. Приховувати тип і версію встановленої CMS і її плагінів, не вказувати їх в коді сторінки.
3. Не використовувати контрафактні версії CMS.
4. Перевіряти всі дані, які користувач може ввести на сторінках сайту або безпосередньо передати серверним скриптам за допомогою запитів.
5. Використовувати мінімум сторонніх скриптів, модулів, розширень.
6. Веб-майстри і адміністратори повинні працювати в безпечному оточенні і виконувати правила безпечної роботи в інтернеті.

ВИСНОВОК

Вибір CMS для розробки web-додатка є важливим і повинен обиратись виходячи з функціональних потреб веб-додатка. Платні CMS більш захищені, але в будь-якому випадку потрібно слідкувати за регулярними оновленнями. Оскільки на сьогодні розглянуті CMS не

входять переліку засобів ТЗІ дозволених для забезпечення технічного захисту державних інформаційних ресурсів, або експертні висновки не є на разі дійсними, є необхідність проведення робіт з перевірки та оцінки ефективності механізму захисту CMS.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
2. Уразливість (інформаційні технології) [Електронний ресурс]. – [Режим доступу]: https://uk.wikipedia.org/wiki/Уразливість_(інформаційні_технології)
3. Система керування вмістом [Електронний ресурс]. – [Режим доступу]: https://uk.wikipedia.org/wiki/Система_керування_вмістом
4. Рейтинг топ CMS за 2018 рік [Електронний ресурс]. – [Режим доступу]: https://it-rating.in.ua/rating-cms-2018-p1
5. Дослідження безпеки CMS-систем 2014 [Електронний ресурс]. – [Режим доступу]: http://www.ruward.ru/sitesecure/sms-survey/
6. Безпека CMS [Електронний ресурс]. – [Режим доступу]: https://yandex.ru/blog/safesearch/120

УДК 004

Зубенко О.В. студентка гр. 125м-17-2
Науковий керівник: Тимофєєв Д.С., ст. викл. кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВИКОРИСТАННЯ МЕТОДИКИ FAIR В ПРОЦЕСІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Вивчення проблем управління ризиками та методів їх вирішення є актуальним і необхідними в сучасному інформаційному суспільстві, через зростання цінності інформації.

До теперішнього часу накопичено достатній досвід і знання з аналізу ризиків, в тому числі і інформаційних. Зазначена проблематика вивчення інформаційних ризиків досить нова в порівнянні з фінансовими, банківськими та іншими ризиками. Але значимість її підвищується в міру зростання залежності суспільства від інформаційних технологій.

Вимоги до управління інформаційними ризиками містяться в міжнародних і вітчизняних стандартах з інформаційної та кібербезпеки, а також обґрунтовані існуючою практикою розвитку інформаційних технологій.

На сьогоднішній день існує безліч інструментальних засобів і методик управління інформаційними ризиками, під якими мається на увазі визначення параметрів ризику, аналіз і оцінка ризику (АОР), а також визначення операцій над ризиками [1]. Часто перед фахівцями компанії для підвищення ефективності вирішення завдань захисту інформації виникає питання про вибір відповідної методики, що задовольняє поточним вимогам інформаційної безпеки підприємства.

FAIR (факторний аналіз інформаційних ризиків) – це міжнародний стандарт кількісного методу оцінки інформаційного ризика.

Посилаючись на основні підходи до менеджменту інформаційними ризиками, що прописані в стандартах Cobit v.5.0, NIST 800-30, ISO/IEC 27000 та ISO/IEC 31000, методика факторного аналізу інформаційних ризиків FAIR, передбачає найбільш повне врахування факторів виникнення інформаційних ризиків [2]. FAIR дозволяє отримати опис достатньої кількісті факторів, що впливають на оцінку ризику та конкретні значення ризику, яким би могли оперувати керівники підприємств.

Основою методики FAIR є аналіз факторів, що впливають безпосередньо на ризик. Аналізуються фактори, що мають вплив на компоненти, що є складовими ризику. Відповідно до зазначеної методики, головними складовими ризику є частота появи інциденту (LEF) та величина збитків від настання зазначеного інциденту (LM) [3]. Кожна з цих складових поділяється на інші фактори: частота появи загрози, вразливість, первинні та вторинні збитки. Використання FAIR передбачає проведення декількох етапів.

Спочатку необхідно визначити область аналізу і що є його метою. Для точного аналізу важлива чітко визначена область. Першою ціллю є визначення сценаріїв ризику, оскільки це є основою для структурування подальшого належного аналізу. Для визначення сценарію, необхідно: провести опис активу (ідентифікація об’єктів оцінки), загрози (частота появи інциденту) і ефекту (стосовно конфіденційності/цілісності/доступності), пов'язаного з аналізованих сценарієм.

Тобто, на першому етапі проводиться ідентифікація активів, загрози (з визначенням її групи та типу), оцінюється ефект загрози, що може бути застосований до інформаційної системи підприємства. Дані фіксуються в таблицю.

Наступний крок – оцінювання кожного зі сценаріїв. До цього етапу входять аналіз частоти появи загрози, існуючих вразливостей та кількісна оцінка факторів можливих збитків.

Частота появи загрози вимірюється з використанням факторів: «мінімальне значення», «найбільш ймовірне значення» та «максимальне значення»

Для оцінки найгіршого варіанту необхідно виконати наступні пункти:

–визначити дію загрози, яка напевно буде результатом найгіршого випадку;

–оцінити величину кожного виду втрат, пов’язаних з дією загрози;

–підсумувати величини всіх видів втрат.

Останнім етапом є розрахунок величини ризику, що відбувається через ідентифікацію сценарія з найвищім показником річних збитків. Інтерпретація результатів проводиться відповідно до запропонованих таблиць методики.

Отже, методика FAIR являє собою детальний аналіз та оцінку ризиків, отриманий результат має конкретні значення ризику, а отже чіткий та доступний для використання. Методика враховує вимоги міжнародних стандартів, а через наявність кількісних характеристик є зручною та актуальною для підприємств, що впроваджують систему управління інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Луцкий М.Г. Базовые понятия управления риском в сфере информационной безопасности / Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – 194 с.

2. Корченко А.Г. Анализ и оценивание рисков ин-формационной безопасности / А.Г. Корченко, А.Е. Архи-пов, С.В. Казмирчук. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

3. Freund J., Jones J. Measuring and managing information risk. A FAIR approach [Текст]: Jack Freund, Jack Jones. – Oxford:Butterworth of Elsevier, 2017. - 391 с.

УДК 004.056.53

Ільман М.В. студент гр. 125-17-2
Науковий керівник: Кручінін О.В. ст. викладач кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ПРИ ВИКОРИСТАННІ ОБЛАДНАННЯ СТАНДАРТУ IEEE 802.11

В роботі розглянута проблематика інформаційної безпеки WI-FI мережі приватного користування. Проведено аналіз безпечності стандарту IEEE 802.11, та комплекси для захисту від несанкціонованого доступу до мережі.

Ключові слова: IEEE 802.11, Wi-Fi, захист інформації, приватна мережа

ВСТУП

З кожним роком кількість інформації в мережі Інтернет зростає за експоненціальним законом, вихід в Інтернет став щоденною необхідністю для кожного користувача цифрової техніки. Особливого поширення набула передача інформації за допомогою стандарту IEEE 802.11(Wi-Fi).

WI-FI - торгова марка Wi-Fi Alliance та загальновживана назва для стандарту IEEE 802.11, передачі цифрових потоків даних по радіоканалах, за допомогою обладнання, що відповідає стандарту IEEE 802.11[1].

Але на жаль, такий спосіб передачі інформації не має належного рівня безпеки передачі інформації. Більшість пристроїв які використовуються у Wi-Fi-мережах мають критичні уразливості, а також функції, які несуть загрозу в стандартному підключенні, без втручання спеціаліста з інформаційної безпеки, та допускають загальновживані паролі.

АНАЛІЗ БЕЗПЕКИ ТИПОВОЇ ПРИВАТНОЇ МЕРЕЖІ WI-FI

Більшість користувачів не мають змоги залучити спеціаліста з інформаційної безпеки, або людину, яка має достатню кваліфікацію в цій сфері, до налаштування своєї домашньої мережі. Так ,в інтернет-магазині «Rozetka» така послуга коштує 399 грн. З точки зору інформаційної безпеки, вони можуть: оновити програмне забезпечення, налаштувати гостьовий доступ, вибрати стандарт шифрування та ввести пароль.[2]

За статистикою Лабораторії Каперського, на кінець 2016 року, третина мереж у світі не мала шифрування за стандартом WPA-2[3]. Статистики на 2018 рік у вільному доступі немає, а сам стандарт WPA-2 є дуже вразливим. На початку 2018 року, з'явився стандарт WPA-3, але станом на листопад 2018, ще немає жодного пристрою, що його підтримують.

Наприклад, виробник WI-FI роутера Netis WF-2411 «запевняє» своїх користувачів, що роутер є безпечним для користування, і для його захисту достатньо ввести пароль від 8 до 63 символів, але не попереджає, що пароль «password» не надає потрібного захисту (рисунок 1).

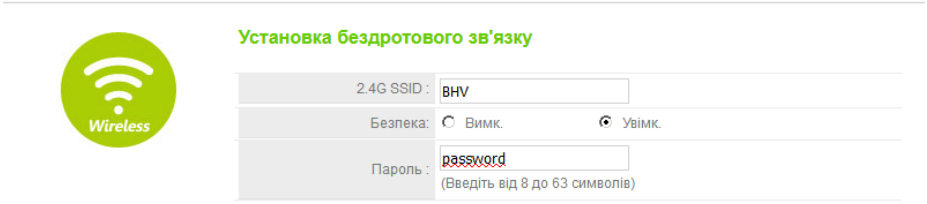


Рисунок 1 – небезпечні налаштування Netis WF-2411

АНАЛІЗ ВІДОМИХ КОМПЛЕКСІВ ЗАХИСТУ WI-FI ВІД НЕСАНКЦІОВАНОГО ДОСТУПУ

Wi-Fi мережі, при відсутності необхідного захисту, є доволі вразливими. Налаштування за умовчанням, які встановленні постачальником маршрутизатору, є не тільки небажаними до використання, але й є потенційною загрозою для конфіденційної інформації користувачів. Постачальникам обладнання слід вносити більшу ясність в своє програмне забезпечення (ПЗ), видаляти з нього зайві функції та доносити до своїх користувачів усю важливість безпечних налаштувань їх мережі.

Для користувачів, які є більш обізнаними у сфері інформаційній безпеки є спеціальні програмні комплекси та апаратно-програмні комплекси, які дозволяють керувати безпекою своєї мережі.

Так, наприклад, комплекси: Mojo AirTight, AirMagnet Enterprise, AirDefense Enterprise та Cisco WIPS - має сенс розгортати лише на великі офіси або цілі будівлі, через їх дороговизну та неможливість налаштування та функціонування при відсутності спеціаліста з інформаційної безпеки. Waidps та Nzyme можна розгорнути, не маючи дорогого обладнання, але в них дуже обмежений функціонал та їх неможливо налаштувати та обслуговувати при відсутності спеціаліста у сфері IT. Avast Free – є антивірусом, який у тому числі може повідомити, про вразливість роутеру, чи про те, що він інфікований, або про інфіковані пристрої в мережі. Також можна відстежити хто підключений до мережі, але ця функція не доступна у фоновому режимі.[4]

На основі аналізу цих продуктів, була складена порівняльна таблиця, яка містить в собі характеристики цих комплексів, та відносну оцінку цих комплексів. Як видно з таблиці 1, жодна з програм не задовольняє потребам користувачів, які не мають змогу розгортати складну та дорогу захисну систему моніторингу.

Таблиця 1

Порівняльна таблиця комплексів для захисту WI-FI мережі

Комплекси/критерії	Аналіз трафіку	Відповідність стандартам	Ціна продукту	Захист та інші корисні функції	Простота роботи	Сумарно балів (0-35)
Mojo AirTight	5	5	4	5	4	23
AirMagnet Enterprise	4	7	2	6	3	22
AirDefense Enterprise	6	5	3	4	2	20
Cisco WIPS	7	7	1	7	1	23
Waidps	3	0	5	3	6	17
Nzyme	2	0	6	2	5	15
Avast Free	1	0	7	1	7	16

Для порівняння використана шкала балів 0-7:

0 – параметр не задовольняє мінімальним вимогам користування;

1 – параметр задовольняє мінімальні вимоги для користування;

7 – найкращий рівень параметру серед представлених вище програм;

ВИСНОВКИ

Більшість Wi-Fi пристроїв без спеціальних налаштувань є достатньо вразливими. Також актуальна проблема оновленням програмного забезпечення в існуючих пристроях.

За результатами проведеного аналізу, жодна з програм не задовольняє потреби приватних користувачів, які не мають змогу розгортати велику та дорогу захисну систему моніторингу. При цьому кожному користувачеві необхідно мати комплекс заходів, які дозволять відстежити більш-менш серйозні атаки. Також доволі гостро стоїть питання наявності кадрів, які б змогли працювати з цими програмно-апаратними комплексами, та сумісного обладнання, тому що розгорнути систему захисту від атак при вже розгорнутій бездротовій мережі може бути занадто дорого.

Таким чином, актуальною є задача розробки заходів захисту для типових умов функціонування приватних мережах при використанні обладнання стандарту IEEE 802.11.

ПЕРЕЛІК ПОСИЛАНЬ

1. https://uk.wikipedia.org/wiki/Wi-Fi
2. https://rozetka.com.ua/support_wifi/p296514/
3. https://securelist.ru/research-on-unsecured-wi-fi-networks-across-the-world/29731/
4. https://help.avast.com/ru/av_free/17/securitynetwork.html

УДК 681
Кочетков К. Д. студент гр. 125м-17-1
Науковий керівник: Рибальченко Ю. П., асистент кафедри безпеки інформації і телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ОПИС ВОЛОКОННОГО АКУСТООПТИЧНОГО ТЕХНІЧНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

Сучасні технології дальньої та локальної кабельних систем зв'язку будуються на основі оптичних систем передачі даних, що пов'язано з перевагами оптичного кабелю в порівнянні з електричним кабелем як транспортного середовища. Таким чином, в будівлях комерційних і державних структур виникає необхідність захисту конфіденційних переговорів у кабінеті керівника, в службових приміщеннях, кімнатах для переговорів та інших виділених приміщеннях від витоку акустичної інформації через оптичні структуровані кабельні системи.

Формування каналу витоку пов'язано з тим, що акустичне поле від носія інформації впливає на оптоволокно штатних інформаційних систем і викликає модуляцію світлового потоку при проходженні через оптоволокно, пасивні елементи або активне волоконно-оптичне обладнання на акустичних частотах, а також при відображенні від неоднорідностей в них. Модуляція світлового потоку в оптоволокні може відбуватися за амплітудою, фазою, поляризації і частоті в результаті впливу акустичного поля на фізичні параметри оптичного волокна. Модульований мовою світловий потік може вийти далеко за межі виділеного приміщення по штатним волоконно-оптичним комунікаціям. Після чого в результаті демодуляції зловмисник може отримати доступ до циркулюючої в установі конфіденційної інформації.

Основними каналами витоку є світлові потоки в оптичному кабелі ліній зв'язку. Всі світлові потоки можна розділити на штатні, пов'язані з фізичною реалізацією протоколу передачі даних, і нештатні, спеціально сформовані порушником для несанкціонованого знімання мовної інформації. Штатні світлові потоки, що формуються, наприклад, при цифрових методах передачі інформації, дозволяють створити канал витоку без порушення роботи всієї системи, так як рівень акустичного впливу на штатний світловий потік незначно зменшує відношення сигнал / шум. До нештатних потоків відносяться будь-які випромінювання, що формуються джерелами світла, несанкціоновано підключені до волоконно-оптичним комунікацій.

Формування акустооптичного (волоконного) каналу витоку інформації практично неможливо без фізичного доступу до оптичного кабелю, що проходить через виділені приміщення. Кабельна мережа повинна бути вільна від активного волоконно-оптичного устаткування на ділянці між порушником і джерелом акустичної інформації, що пов'язано з відновленням форми штатних сигналів і придушенням шумових складових випромінювання в активному обладнанні. Між порушником і джерелом акустичної інформації повинен розташовуватися оптичний кабель з пасивними оптичними елементами, які не змінюють істотно модуляцію світлового потоку. До пасивних оптичних елементів, крім оптичного кабелю, відносяться розетки, адаптери, подільники, атенюатори. Треба відзначити, що подібна структура оптичної кабельної мережі є найбільш перспективною для абонентського доступу і активно розвивається у вигляді технології пасивних оптичних мереж.

Реалізація каналу витоку вимагає застосування технічних засобів підключення до кабелю і реєстрації оптичного випромінювання. Підключення здійснюється через штатні роз'ємні з'єднання, які використовуються для з'єднання окремих частин мережі між собою, для приєднання до стаціонарних (optical line terminal, OLT) і мережевих (optical network terminal, ONT) терміналів. З'єднання роз'єднується і в нього вставляється вставка з введенням зондуючого випромінювання і відведенням частини випромінювання. Інший спосіб приєднання полягає в застосуванні відгалужувача випромінювання на макровигині оптичного

кабелю. Всі запропоновані способи не вимагають застосування спеціальних технічних засобів, поширення яких регламентовано нормативними документами - такі пристосування використовуються при монтажі оптичної мережі. Ще один спосіб використовує нештатний розрив кабелю з вставкою відгалужувача шляхом зварювання волокон.

Оптична схема підслуховування може бути реалізована кількома способами. По-перше, можуть бути застосовані спеціальні зондувальні джерела світла, які не передбачені штатної мережею. Зондувати можна методом відображення або пропускання зондуючого променя крізь місце модуляції. В цьому випадку можна поєднати його з приймально-передавальним випромінюванням. По-друге, для підслуховування може бути використано штатний випромінювання, яке застосовується для передачі трафіку всередині мережі.

Небезпека каналу витоку можна визначити по ефективності акустичної модуляції в місці розташування джерела інформації. Акустичне поле викликає різні види модуляції світлових потоків в оптичному волокні. Підбираючи параметри демодуляції світлового потоку (амплітуду, фазу, поляризацію або частоту) завжди можна досягти дуже високої ефективності каналу витоку акустичної (мовної) інформації. Ще одна небезпека пов'язана з доступністю монтажного обладнання, яке може бути використане як спеціальний технічний засіб акустичної розвідки. Наприклад, для мовного зв'язку між монтажниками мережі використовуються волоконно-оптичні телефони, які дозволяють при прямому приєднанні до волокна здійснювати звуковий зв'язок на відстані більше 200 км. Волоконно-оптичні телефони можуть підключатися до оптичного кабелю без його розриву з допомогою макровигину оптоволокна. Для підслуховування може бути використаний вимірювач рівня зворотного відбиття, призначений для контролю якості полірування одномодових волоконно-оптичних з'єднувачів і вимірювання рівня зворотного відбиття від інших компонентів ліній зв'язку. Ще більші можливості має рефлектометр - основний пристрій контролю стану оптичного кабелю. Названі прилади є загальнодоступними і широко використовуються при монтажі оптичних кабельних систем, що підвищує небезпеку їх застосування в каналі витоку [1].

ПЕРЕЛІК ПОСИЛАНЬ

1. Trojer E., Dahlfort S., Hood D. and Mickelsson H. Current and next-generation PONs: A technical overview of present and future PON technology. – Ericsson Review, 2008, №. 2, p. 64.
2. . LamC. Passive Optical Networks: Principles and Practice. – San Diego, California.: Elsevier, 2007.
3. Каток В.Б., Руденко І.Е., Однорог П.М. Волоконно-оптичні лінії зв’язку. – Київ, 2016

УДК 681.518.54

Рогалєва М.В. студентка гр. 125м-17-1
Науковий керівник: Святошенко В. О. ст. викл. кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

АТАКИ НА САЙТИ ТА ЯК ЇМ ПРОТИДІЯТИ

Атаки на сайти - вчинення протиправних дій щодо веб-сайтів спрямованих на отримання конкурентних переваг шляхом злому, зараження шкідливим кодом, блокування доступу (з надалі вимогою викупу), крадіжку конфіденційних даних, виведення з ладу програмного забезпечення.

Веб-сайти - це інформаційний актив і вид власності. Він може піддаватися атакам зловмисників з різними цілями. Сайт завжди повинен бути доступним і це робить його вкрай уразливим.

Перед атакою на сайт кіберзлочинець вивчає його на предмет вразливостей. Вони, в свою чергу, бувають декількох типів: Уразливості коду сайту. З'являються такі уразливості через помилки або недостатньої опрацювання питань безпеки програмістами, що створюють ядро і розширення сайту. При наявності подібних вразливостей хакер може впровадити свій код в виконувані скрипти, запити до бази даних (SQL-ін'єкції), поштового сервера сайту (email-ін'єкції), або в сторінку, яку користувач відкриває в своєму браузері, з метою крадіжки його особистих даних, включаючи паролі (міжсайтовий скриптинг). Дуже рідко весь код сайту пишеться з нуля, набагато частіше використовується одна з існуючих CMS - систем управління контентом, а також різні модулі та розширення, що додають потрібну функціональність. Частина з них поширюється безкоштовно, за інші потрібно заплатити. Зламавши таке платне розширення, зловмисник додає в нього шелл-код, що відкриває доступ до сайта або веб-сервера, і пропонує для скачування вже безкоштовно. Також, вразливим може бути і хостинг-провайдер. На одному сервері можуть розміщуватися десятки і сотні сайтів, і якщо він налаштований неправильно, то, зламавши один сайт, хакер здатний отримати доступ і до інших.

Наявність будь-якого типу вразливості веб-сайту призводить до атак, метою яких в більшості випадків стає повний несанкціонований доступ до вмісту сайту. Отримання його залежить від характеру уразливості - при SQL-ін'єкції шляхом різних запитів до бази даних отримують логіни і паролі всіх користувачів, включаючи адміністратора. Маючи ж права адміністратора, з зараженим сайтом можна робити що завгодно. Іноді зловмисники не втручаються в нормальну роботу, обмежуючись крадіжкою клієнтської бази і даних користувачів, іноді знищують або підміняють вміст, або доповнюють функціональність відповідно до власних потреб - розміщують рекламні банери, посилання на порнографічні та поширюють заборонену інформацію ресурси, фішингові сайти, або для межсайтовой підробки запиту , коли від імені користувача, який зайшов на сторінку і має аккаунт на іншому ресурсі (наприклад, електронну платіжну систему) робиться запит на переказ грошей злочинцеві.

DDoS-атаки досить відомі і поширені. Коли в новинах зустрічається новина, що такий-то сайт недоступний, найчастіше це результат саме DDoS-атаки. Їх мета - не потрапити в систему, підмінити контент або вкрасти чужі дані, зробити сайт недоступним на деякий час. Після цього власників сайту, як правило, шантажують і вимагають гроші за зупинку атаки. Здійснюється DDoS-атака одночасним посиланням запитів з безліч комп'ютерів ботнету. Перевантажуючи сервер потоком безглуздих повідомлень, атакуючий робить його недоступним для звичайних відвідувачів.

Інтернет сайти на популярних CMS зламують масово з метою зараження через типові уразливості. Що ж стосується DDoS-атак, то їх роблять на замовлення і тут є конкретні групи ризику. Наприклад, дуже часто атакують бізнес який залежить від інтернету. Зловмисники починають атаку і пропонують власнику відкупитися. За статистикою найчастіше атакують: купонні сервіси, платіжні системи, інформаційні агрегатори, електронну комерцію, ігри та

ігрові майданчики, інші Веб-сторінки банків і електронних платіжних систем зламують з метою крадіжки грошей, сайти комерційних компаній ламають заради клієнтської бази і створення проблем конкуренту, або шантажу, вимагаючи гроші за відновлення нормальної роботи, сайти урядових органів і громадських організацій атакуються ідеологічними противниками.

Основним джерелом загрози для сайту є його власний код, написаний недбало, з помилками, без урахування строгих правил безпеки, а також використання застарілих, або викачаних з піратських сайтів модулів, розширень і плагінів. Інша серйозна проблема - неправильне адміністрування. Надаючи користувачам надмірно широкі права, дозволяючи їм завантажувати на сайт файли без належної перевірки, адміністратор фактично відкриває ворота для троянів, бекдор та іншого шкідливого ПЗ. Третє джерело небезпеки - погані паролі. Ще одна не пов'язана безпосередньо зі створенням і роботою сайту загроза - вміст як таке. Рушійною силою багатьох, в першу чергу DDoS-атак є помста. Від них не рятує правильний код і надійне адміністрування - атака йде ззовні. Зробити сайт стовідсотково стійким до будь-яких атак неможливо. Можна лише ускладнити злочинцям досягнення їхніх цілей. Зрештою, атака на сайт вимагає часу і грошей, і якщо передбачувана вигода або збиток противника виявиться менш витрати на спробу злому - хакер переключиться на більш привабливу мету.

Щоб не допустити атаку на сайт, потрібно використовувати, при створенні лише надійні, перевірені двигуни, а якщо замовляється свій, то доручати його написання команді досвідчених професіоналів. При використанні готових систем управління контентом, регулярно їх оновлювати - більшість поновлення призначені якраз для усунення чергових виявлень уразливості. Не можна використовувати старі, та неоновлювані CMS - дірки в їх безпеки ніким не закриваються і добре відомі хакерам, які не забаряться ними скористатися. Те ж саме стосується будь-яких додатків і розширень. Безкоштовні завантажування тільки з сайтів офіційних розробників, їх потрібно своєчасно оновлювати, платні - купувати, або відмовитися від їх використання. За умовно-безкоштовне скачування з піратського сайту в кінцевому рахунку доведеться заплатити набагато більше, коли знадобиться відновлювати як вміст, так і репутацію в очах пошукових систем, які ігнорують сайти, що містять нерелевантні посилання і поширюють заражені файли. Необхідно чітко розмежувати права різних категорій користувачів. Ніхто не повинен мати більше можливостей, ніж необхідно. Паролі для адміністраторів і привілейованих груп користувачів повинні бути складними. Бажано використовувати різні програми і утиліти, що підвищують безпеку. Непогано також перевірити сайт спеціальними програмами пошуку вразливостей, або, якщо надійність важлива і фінанси дозволяють, доручити задачу професіоналам. При захисті від потужних DDoS-атак частіш залишається саме перечекати, поки вона припиниться. Замовники DDoS-атак рідко мають у своєму розпорядженні власні ресурси для її проведення, і змушені платити хакерам - власникам ботнетів (мереж заражених комп'ютерів, з яких і ведеться атака). Відповідно, потужна атака коштує чималих грошей, і рідко триває довше декількох днів. А щоб знизити ймовірність DDoS-атак, не варто розміщувати контент, образливий для великих груп людей або впливових структур, здатних помститися. Нарешті, варто регулярно створювати резервні копії сайту, щоб в разі серйозних проблем швидко його відновити.

ПЕРЕЛІК ПОСИЛАНЬ

1. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13.
2. Выполнение произвольного кода в Opera http://www.securitylab.ru/news/391365.php
3. Отчет по уязвимостям. Валерий Марчук http://www.securitylab.ru/analytics/358113.php
4. Обход ограничений безопасности MS Internet Explorer http://www.securitylab.ru/vulnerability/355316.php
5. Обзор уязвимостей http://www.xakep.ru/post/47037/default.asp

УДК 004.056.53

Руденко С.С. студент гр. 125м-17-2
Науковий керівник: ст. викладач Святошенко В.О.
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ДАНИХ НА КОМП'ЮТЕРІ

Проблема захисту інформації є далеко не новою. Вирішувати її люди намагалися з давніх часів. Втрата недокументованих електронних даних спричиняла необхідність повторного виконання необхідної обробки інформації. В деяких випадках втрата вихідних даних робила неможливою повторну обробку інформації, а отже, і втрату важливих результатів.

Існує дві найпоширеніших видів ідентифікації: парольна ідентифікація та апаратна ідентифікація.

Методи аутентифікації умовно можна поділити на однофакторні та двофакторні. Однофакторні методи діляться на: логічні, ідентифікаційні та біометричні.

Відбитки пальців стали дійсно біометричним параметром, що найбільше широко використовується в усім світі і використовується більш ніж у 50% усіх сучасних біометричних систем. Біометрія, як наука вивчення математичних або статистичних властивостей у фізіологічних і поведінкових людських характеристиках, широко використовується у сфері захисту інформації. Використання відбитків пальців в якості біометрії є одним з найстаріших методів автоматизованої ідентифікації особи і водночас найбільш поширеною в наш час. До числа факторів, які сприяють поширенню використання систем такого типу можна віднести: незначні розміри та вартість апаратури для обробки зображень відбитків пальців, високопродуктивне апаратне забезпечення, степінь та швидкість розпізнавання, що відповідають вимогам програмного забезпечення, різкий ріст та розвиток мережних технологій та Інтернету, а також усвідомлення необхідності простих, базових методів захисту та безпеки інформації.

Отже, суть технічної проблеми полягає в розробці нового підходу до обробки зображення відбитка пальця з метою ідентифікації особистості, та обмеження доступу до комп'ютерних ресурсів.

ВИЗНАЧЕННЯ ТРЕНДУ ПОТОКІВ ЛІНІЙ НА ВІДБИТКУ ПАЛЬЦЯ

Після оцінки міри регулярності зображення по всіх осях, вибираються максимальні величини з пар R_V, R_H, R_L, R_P і, як їх геометрична сума, визначається напрям максимальної регулярності, відносно якого задається еталонна орієнтація. Кут нахилу зображення відносно осі X визначається як:

$$\varphi = arctg(\max\{R_V, R_H\} + \max\{R_L, R_P\})$$

Якщо в даній зоні зображення присутні лише вертикальні або лише горизонтальні складові, то кут нахилу не обчислюється, а приймається рівним 90° або 0°, відповідно. За відсутності ліній відбитку у виділеній зоні вектор кута нахилу не будується взагалі.

ПОБУДОВА ГЛОБАЛЬНОГО ОПИСУ ВІДБИТКУ ПАЛЬЦЯ

При аналізі структури з метою здобуття додаткових інформативних ознак проводиться декомпозиція оцінок складності, регулярності і кута орієнтації на часткові оцінки, що характеризують окремі фрагменти зображення. Для обліку зв'язності ліній сусідніх фрагментів логічно ці фрагменти вибирати з перекриттям. Для кожного фрагмента розраховується кут тенденції орієнтації ліній і будується відрізок під розрахованим кутом.

Отримана матриця величин кутів орієнтації ліній у фрагментах і їх відображення у вигляді орієнтованих відрізків є портретом регулярності елементів текстури (ПРЕТ), представленим на рис. 1. Від розмірів фрагментів залежить об'єм ПРЕТ і його детальність. Відмінною особливістю портрета є здатність повторення геометрії рисунка відбитку із збереженням основних ознак, прийнятих в криміналістиці.

Графічне зображення відбитку є матрицею розміром *256×256* точок (пікселів). Для побудови портрета регулярності даний малюнок розбивається на зоні розміром *16×16* пікселів, для кожної з яких визначається кут нахилу і будується відповідний відрізок. Таким чином "гладке" зображення відбитку замінюється набором дискретних відрізків. Для згладжування і зменшення погрішності при аналізі вибиралися зони, що перекриваються, розміром *32×32*, але відрізок будується для елементу зображення розміром *16×16*.

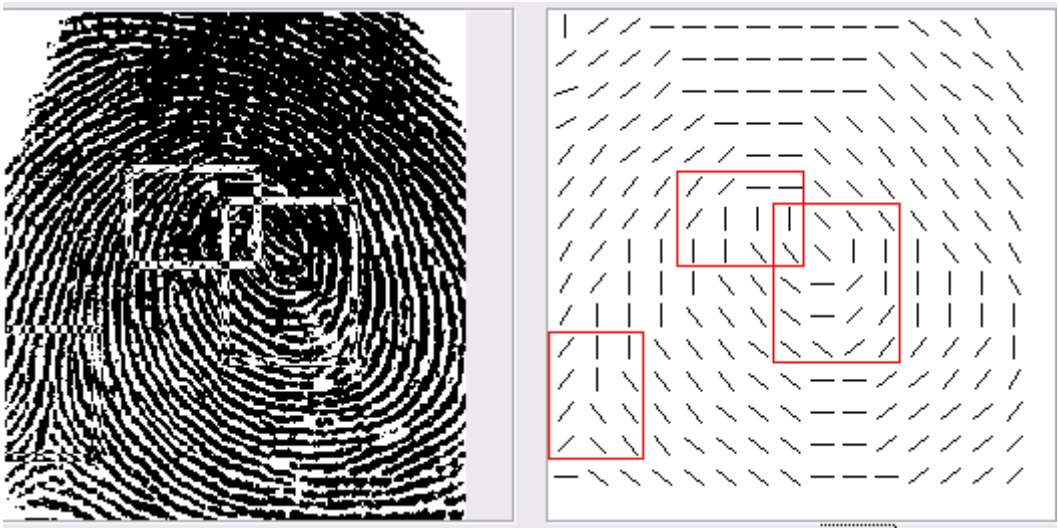


Рисунок 1 - Отримання портрета відбитку

В результаті проведеного перетворення графічного зображення відбитку з вибраною кількістю фрагментів отримано *256 (16×16)* зон значень кута нахилу і портрет регулярності. Для здобуття ще ближчого дискретного еквіваленту вихідного зображення відбитку використовується алгоритм інтерполяції, який дозволяє поєднати відрізки на межі зон, що є сусідніми. ПРЕТ відбитку несе в собі стислу інформацію про його структуру. Тому його можна використовувати для попередньої ідентифікації, результатом якої має бути одне з двох тверджень:

- ПРЕТ відбитку, що пред'являється, корелює з відповідним еталонним ПРЕТом;
- кореляція між ПРЕТамі відбитку, що пред'являється, і вказаного еталону не спостерігається.

У першому випадку для подальшої точної ідентифікації необхідно порівняти структуру пред'явленого відбитку з еталонним. Причому для скорочення часу повної ідентифікації необхідно порівнювати структури найбільш інформативних фрагментів невеликих розмірів.

У другому випадку формується негативний результат ідентифікації і подальшого порівняння не відбувається. Як показує величезний досвід криміналістики, найбільш інформативними, з точки зору ідентифікації, є фрагменти з яскраво вираженими порушеннями регулярності папілярних ліній, що в ПРЕТ відповідає різкій відмінності значень кутів нахилу ліній в сусідніх зонах. Для автоматичного знаходження таких зон паралельно з формуванням ПРЕТ формується його загрублений варіант, в якому одним числом кодується не конкретне значення кута, а деякий інтервал кутів.

Приховувати свої папки та файли можна, використовуючи вбудовані можливості Windows - для цього достатньо у властивостях відповідних об'єктів включити атрибут "Прихований". Приховані таким чином папки та файли не будуть бачити в провіднику іншим користувачам системи, але лише за умови, що у властивостях містять їх батьківських папок включений прапорець «Не показувати приховані файли і папки". В принципі, цього може виявитися достатньо для захисту своїх даних від найбільш непідготовленою аудиторії. Однак приховані подібним чином об'єкти будуть видимі в додатках, які не використовують стандартний діалог для відображення файлів і папок (FAR, Total Commander і т.п.), тому подібний захист більш ніж ненадійна. Тому була виявлена необхідність розробки програмного

продукту призначеного для верифікації користувача по запропонованому зображенню відбитку пальця. Оцінюючи проведену роботу по розробці програмного продукту можна відзначити, що методи і алгоритми, використовувані при побудові портрета відбитку, при виділенні інформативних зон, при виділенні ознак, при ідентифікації відбитку, при блокуванні папки, а також розлокуванні папки працюють ефективно і по багатьом параметрам не поступаються закордонним аналогам. Результати аналізу роботи програми показали, що можливе введення додаткових методів порівняння, та механізмів захисту даних. Це дозволить збільшити достовірність результату ідентифікації, та більш надійніше захистити дані на комп'ютері.

ПЕРЕЛІК ПОСИЛАНЬ

1. А.И. Гороховский, Харьков А.М. Автоматическая идентификация по отпечатку пальца. В кн. «Приборостроение 2000», Калуга, стр. 238-243.

2. А.И. Гороховский, Кожемяко В.П., Шепетко А.Ф. Структурно-статистическая идентификация текстур. В кн.: Автоматизированные системы обработки изображений: Тез. докладов II Всесоюз.конф., 1986, Львов.

3. Чередниченко В. Б. Біометричні методи у системах захисту інформації.

4. С. Бармен. Розробка правил інформаційної безпеки / Бармен С. [Пер. з англ.] – М.: Вид-во "Вільямс", 2002. — 208 с.

УДК 004

Ковальова Ю.В., аспірант кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка,
Сєрак Т.Г., студентка гр. 125м-17-2 кафедри безпеки інформації та телекоммунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВПЛИВ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА КІБЕРБЕЗПЕКУ

Розвиток інформаційного простору передбачає зростання числа кібератак, де основна загроза спирається на людський фактор. У цій роботі аналізується сучасний стан впливу інформаційної безпеки та соціальної інженерії на загальну систему.

У сучасному світі інформаційні технології отримують ряд тенденцій, спрямованих на розвиток та розширення власних ресурсів. Це викликано перенесенням бізнес-додатків в Інтернет. Виникнення "хмарної" інфраструктури (хмарних обчислень) та "програмного забезпечення як сервісу" (SaaS) істотно знижують витрати компаній на обладнання та обслуговування послуг, що використовують інформаційні технології. Розвиток інформаційного простору передбачає наступний фактор вразливості - несанкціонований доступ до мережі та збільшення кібератак.

Незважаючи на динамічний розвиток сектора кібербезпеки в країнах світу, основним аспектом шкідливих нападів на інформаційні системи залишається людський фактор. У зв'язку з цим в ряді країн соціальна інженерія стала широко поширеною як метод несанкціонованого доступу.

Сьогодні Україна перебуває у критичній економічній ситуації, на яку сильно впливає політична ситуація та міжнародна орієнтація. Тому сектор інформаційної безпеки є вразливим, як ніколи раніше. Зважаючи на військову та політичну ситуацію, особливу увагу слід приділити стратегічним цілям, на які впливає фактор соціальної інженерії.

У зв'язку з цим набуває ступеня важливості вразливості мереж енергопостачання, оскільки порушення цілісності цих мереж завдає величезний економічний та соціальний збиток державі в цілому.

Міжнародне співтовариство в галузі інформаційної безпеки протягом останнього десятиліття приділяє особливу увагу підвищенню обізнаності про соціальну інженерію як загрозу, яка має значну небезпеку для інтелектуальної власності та інформаційних ресурсів.

В контексті інформаційної безпеки соціальна інженерія - це метод психологічного маніпулювання, який використовується для видалення конфіденційної інформації для подальших шкідливих атак. Хакери часто використовують методи соціальної інженерії для отримання доступу до фінансової інформації та звітності. Використання Інтернету у всіх сферах нашого життя підвищує можливості соціальної інженерії (1).

Дослідники відзначають, що великі бізнес-структури зазвичай покладаються на технічні засоби захисту від нападів. У той же час підготовка персоналу практично залишається без уваги, щоб атакуючі могли отримати доступ до внутрішніх мереж компаній, використовуючи методи соціальної інженерії.

Мета соціальної інженерії полягає у заохоченні людей робити певні дії, які, за звичайних умов, вони ніколи б не робили, наприклад - розголошення їх конфіденційної інформації, направлення на невідомі сайти та підозрілі посилання. Вся система соціальної інженерії базується на тому, що людина є найслабшою ланкою в будь-якій системі інформації та кібербезпеки. Тому у випадку, якщо з технічними методами хакери не можуть отримати конфіденційну інформацію, вони безпосередньо впливають на користувача - найслабшого місця в системі інформаційної безпеки.

Взаємозалежність нинішньої політичної та економічної ситуації в Україні безпосередньо сприяла збільшенню кількості кібератак за останні 2 роки. Кібернапади на Україну стали

важливою частиною гібридної війни. Комп'ютерна аварійна команда України в 2014 році зафіксувала наступну кількість нападів:

- на державні установи - 124
- на комерційні заклади- 42
- в іноземних комерційних установах в Україні - 29
- в іноземних державних установах в Україні - 11 (2).

Україна стала абсолютним лідером у внутрішніх і зовнішніх кібер-загрозах в Європі. В останні роки Україна неодноразово орієнтувалася не тільки на невеликі шахрайства, але й на великі кібер-операції.

Україна займає п'яте місце в світі (і перше в Європі) на ризик зіткнення з веб-загрозами. За даними Kaspersky Security Network, з липня-вересня 2015 року третина (33,7%) українських користувачів Інтернету зіткнулися з загрозами, спричиненими Інтернетом (3).

Серед жертв Турли - однієї з найбільших кампаній в галузі кібер-шпигунства, яка функціонує вже понад 8 років, знайшли комп'ютери українських чиновників. Група, яка знаходиться за Турлою, заразила сотні комп'ютерів у більш ніж 45 країнах світу, що належать, зокрема, державним установам, посольствам, військовим, дослідницьким центрам та фармацевтичним компаніям. Метою кіберзлочинців є збір необхідних або конфіденційних даних з комп'ютера жертви.

Також українці були серед жертв таких компаній, як Cosmic Duke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy та Red October (4).

Успішна реалізація технології Smart Grid сприяла розробці програм Smart City, Smart Water, Smart Lighting, Smart Utility у більшості розвинених країн світу. На тлі вибухонебезпечного характеру розвитку технології на перший план висувається проблема кібербезпеки та захисту інформації в інтелектуальних мережах, що забезпечують підтримку населення. Прогнозована на конференції (5) вразливість інтелектуальних мереж, побудована на базі інтелектуальних лічильників, була підтверджена 23 грудня 2015 року, коли споживачі Прикарпаттяобленерго (6) були піддані відключенню в результаті потужної кібератаки.

23 грудня відбулися карпатські магістральні відключення. Енергетична компанія "Прикарпаття-Обленерго" повідомила про невдачу, внаслідок чого проблеми з постачанням електроенергії спостерігались у всьому регіоні, включаючи Івано-Франківськ. Близько 700 тисяч споживачів залишалися без електрики протягом декількох годин. Прес-служба Прикарпаттяобленерго повідомила, що причиною великомасштабної катастрофи, ймовірно, є втручання неавторизованих осіб у роботу пульта дистанційного керування - системи моніторингу та контролю автоматичного енергетичного обладнання. Напад на Прикарпаттяобленерго був першим випадком історії, коли кібернападу вдалося зупинити енергопостачання. "Вперше ми маємо докази і можемо пов'язувати певну шкідливу програму з невдалою системою", - заявив старший науковий співробітник Trend Micro Кайл Вілойт. Хакери використовують шкідливе програмне забезпечення на платформі BlackEnergy, надаючи їм можливість отримати доступ до мережі та встановлювати програму KillDisk, яка може видаляти та перезаписувати файли. BlackEnergy вірус увійшов до системи в результаті виявлення зараженого додатка Microsoft Word. Після кібератаки послідувало телефонне "затоплення" в ряді енергокомпаній технічної підтримки.

Якщо такі жорсткі звинувачення доведені, це змінить думку про ефективність "хакерської війни". Це буде ознакою того, що кібернапад може бути використаний у військових цілях (7).

ВИСНОВОК

Цей факт вказує на потенційну вразливість мережевої інформаційної інфраструктури енергетичних та комунальних підприємств. Цей приклад проникнення енергетичної системи є прикладом важливості аспектів соціальної інженерії.

Енергетичні об'єкти виконують стратегічну роль у країні, тому необхідно мінімізувати вплив людського фактора в ці системи, щоб забезпечити безпеку та цілісність інформації, що

поширюється на об'єктах. У зв'язку з цим використання стає актуальним технологіями Smart Grid в секторах енергетики та комунальних послуг.

ПЕРЕЛІК ПОСИЛАНЬ

1. Департамент родственної безпеки, доповідь про мистецтво соціальної інженерії - 18 січня 2016.

2. CERT-UA, Комп'ютерна аварійна команда України.

3. Форум з кібербезпеки, Лабораторія Касперського, Угорщина - 20 листопада 2015.

4. М. Ярова. 8 тез про кібербезпеку в Україні - 2015.

5.Ю. Почта. Українська науково-практична конференція "Системний аналіз. Комп'ютерні науки. Менеджмент".

6. "Вашингтон Пост", хакери, які підозрюються в нападі, які затьмарили частини України - 5 січня 2016.

7.Хосе Пальярі. CNN-Tech. Страшні питання в енергетичній мережі України, 18.01.2016.

УДК 004.773.3

Ушенко М.С. студент гр. 125м-17-2
Науковий керівник: Галушко С.О. ст. викл. кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ЗАХИСТ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ

Із зростанням ролі електронної пошти збільшуються і потреби в управлінні нею - це завдання в даний час актуальне, як ніколи. Електронна пошта для більшості компаній є основним засобом комунікації. Переписка необхідна як для спілкування всередині самої компанії, так і для обміну даними з партнерами, клієнтами, постачальниками, державними органами і т.д. Тим більшого значення набуває ефективна корпоративна система управління електронною поштою - надійна, з високою пропускною здатністю, оснащена засобами контролю і відсіву небажаних повідомлень. Адміністраторам поштових систем доводиться постійно боротися зі спамом, вірусами та хакерськими атаками.

Електронна пошта має численні перевагами, але саме через ці достоїнства виникають основні ризики, пов'язані з її використанням. Наприклад, доступність електронної пошти перетворюється в недолік, коли користувачі починають застосовувати пошту для розсилки спаму, легкість у використанні та безконтрольність призводить до витоку інформації, можливість пересилання різних форматів документів - до поширення вірусів і т.д.

З огляду на описані вище ризики, пов'язані з використанням електронної пошти, організаціям необхідно вжити відповідних заходів для захисту від них. Підхід до захисту повинен бути всебічним і комплексним - необхідно поєднувати організаційні заходи з використанням відповідних технічних засобів. До організаційних заходів належать розробка та впровадження в компанії політики використання електронної пошти. Технічні засоби повинні забезпечити виконання даної політики як за рахунок моніторингу поштового трафіку, так і за рахунок адекватного реагування на порушення.

Відомі численні приватні рішення для аналізу трафіку або його суцільного сканування, фільтрації контента, блокування спаму, генерування попереджень про небезпеку, підтримки певних політик, балансу завантаження поштових серверів і т. д. Однак рішень, які об'єднують всі необхідні інструменти і працюють на різних платформах з різними поштовими системами, не так багато. Вважається що якісному антиспамовому продукту повинні бути притаманні такі основні властивості:

- інтероперабельність (здатність до взаємодії) - система управління легко вбудовується в існуючу інфраструктуру підприємства, здатна працювати в гетерогенному середовищі і має можливості масштабування;
- мінімальний вплив - система не повинна додавати ніяких нових ризиків, явних чи прихованих вимог додаткових ресурсів;
- засоби спостереження - вся інформація про стан системи і про те, як вона використовується, повинна бути під рукою у адміністратора;
- захист - система повинна вміти виявляти загрози в реальному часі і самостійно ліквідувати їх без втручання адміністратора; це стосується і вірусної загрози та спроб хакерських атак;
- надійність - мета роботи системи управління - підвищити ступінь готовності ресурсу і пом'якшити вплив відмов, певним чином обробляючи аварійні ситуації;
- прийнятна окупність - щоб отримати схвалення осіб, що дають згоду на інвестиції, система повинна мати мінімально можливу вартість.

Прикладом комплексного додаткового рішення може служити ПО, розроблене компанією Postini. Продукт розташовується між каналом Internet і внутрішньою мережею організації. він

не замінює собою основний поштовий сервер і не вносить жодних змін в сховище повідомлень.

Додаток обробляє SMTP-трафік на рівні сесії і не вимагає будь-якої інтеграції з самим поштовим сервером. При цьому виявляються поштові атаки, спам і віруси. Виконується також збір детальної статистичної інформації, що дає змогу аналізувати поштовий трафік компанії.

Компанії, які спеціалізуються в області боротьби зі спамом, добре знають більшість прийомів і вивертів спамерів. Тому в середньому рівень очищення потоку пошти у них вище, ніж можуть досягти адміністратори звичайних компаній, а відсоток відсіву потрібних ділових листів - менше. Вони швидко виявляють нові прийоми спамерів і проводять нейтралізуючі заходи. Така послуга називається спам-аутсорсинг.

Найбільш ефективним заходом перешкоди витоків інформації електронною поштою є її шифрування. В цьому випадку, навіть якщо зловмисник отримав доступ до пошти, прочитати її він не зможе.

При цьому методі використовуються два ключа - публічний і приватний, за допомогою яких листи шифруються і дешифруються. Одержувач повинен знати публічний ключ, для цього відправник може опублікувати Private key онлайн, наприклад на своєму сайті, або розіслати звичайним листом всім потенційним одержувачам.

ВИСНОВКИ

В даний час діяльність компаній все більше залежить від електронної пошти. Зручність і практичність електронної пошти очевидні. Однак не можна не враховувати проблеми, які виникають у зв'язку з її неконтрольованим використанням. Наслідки для компаній можуть бути непередбачуваними.

Таким чином, всі перераховані вище факти ще раз підтверджують необхідність застосування в системах безпеки корпоративних мереж систем контролю вмісту електронної пошти, які здатні не тільки забезпечити захист системи електронної пошти і стати ефективним елементом управління поштовим потоком, але і значно підвищити ефективність діяльності підприємства чи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1.Корпоративная электронная почта: контроль, защита, надежность [Електронний ресурс] Режим доступу:
https://itc.ua/articles/korporativnaya_jelektronnaya_pochta_kontrol_zashhita_nadezhnost_10992/

2.Безопасность систем электронной почты [Електронний ресурс] Режим доступу: http://citforum.ck.ua/security/internet/email/article1.6.200355.html

3.Защита корпоративной почты [Електронний ресурс] Режим доступу: https://efsol.ru/articles/protection-of-corporate-e-mail.html

4.Безопасность электронной почты: шифрование писем [Електронний ресурс] Режим доступу: https://habr.com/post/190130/

Секція 3 – Телекомунікації та радіотехніка

УДК 621.396.9

Сіданченко В.В., студент гр. 172м-17-1
Науковий керівник: Гусєв О.Ю., к.ф-м.н., професор кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ТЕХНОЛОГІЯ АТМОСФЕРНИХ ОПТИЧНИХ ЛІНІЙ ЗВ'ЯЗКУ (АОЛЗ) І НАПРЯМКИ ЇЇ РОЗВИТКУ

Технологія АОЛЗ (її також називають FSO – Free Space Optics, БОКЗ - Бездротовий Оптичний Канал Зв'язку, або ЛАЛ - Лазерна Атмосферна Лінія) ґрунтується на передачі даних модульованим випромінюванням в інфрачервоній частині спектра через атмосферу і їх подальшим детектуванням оптичним пристроєм. При цьому в якості випромінювача зазвичай використовуються інфрачервоні лазери класу 1 або 1М (до лазерів 1-го класу відносять повністю безпечні лазери, вихідне випромінювання яке не представляє небезпеки при опроміненні очей і шкіри). Для низькошвидкісних комунікацій на невеликі відстані можуть використовуватися світлодіоди. В якості приймача використовуються лавинні або кремнієві фотодіоди (рис.1) [1].

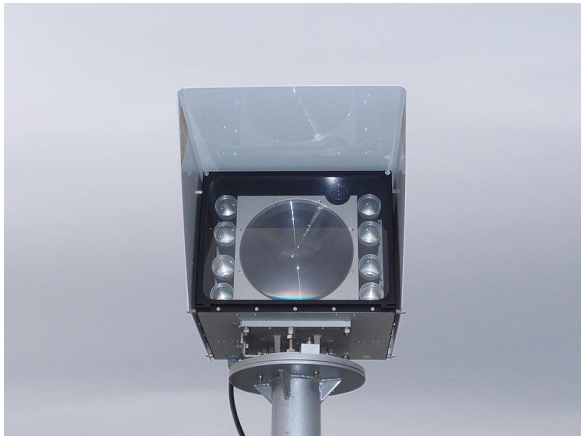


Рисунок 1 - Восьмипромінний лазерний приймач для атмосферного оптичного зв'язку. Швидкість передачі - до 1 Гбіт / с на відстані близько 2 км. Великий диск в центрі - приймач, малі диски зліва і справа - передавачі, гурток зверху справа - вікно оптичного монокуляра для виставлення двох блоків по загальному променю

В основі бездротових оптичних систем лежать технології організації високошвидкісних каналів зв'язку за допомогою інфрачервоного випромінювання, які роблять можливою передачу даних (текстові, звукові, графічні дані) між об'єктами через атмосферний простір, надаючи оптичне з'єднання без використання скловолокна.

Технологія ґрунтується на передачі даних модульованим випромінюванням в інфрачервоній частині спектра через атмосферу. В якості передавача виступає потужний напівпровідниковий лазерний діод. Інформація надходить в приймальний модуль, в якому кодується різними перешкодостійкими кодами, модулюються оптичним лазерним випромінювачем і фокусується оптичною системою передавача в вузький лазерний промінь і передається в атмосферу .

На приймаючій стороні оптична система фокусує оптичний сигнал на високочутливий фотодіод (або лавинний фотодіод), який перетворює оптичний пучок в електричний сигнал. Далі сигнал демодулюється і перетворюється в сигнали вихідного інтерфейсу.

Система АОЛЗ може бути розгорнута дуже швидко, якщо є доступ до електроенергії і є можливість закріпити приймально-передавач на стабільній платформі. Це дозволяє

використовувати систему також для тимчасових рішень таких як, наприклад, масові заходи або зустрічі в місцях, де відсутня широкосмуговий доступ в інтернет.

Однак система може бути також використана і для забезпечення постійного зв'язку на невеликих відстанях (не більше 4-5 км) в міських районах використовую архітектуру точка-точка.

До основних переваг атмосферних оптичних ліній зв'язку відносяться:

- висока пропускна здатність і якість цифрового зв'язку. Сучасні FSO-рішення можуть забезпечити швидкість передачі цифрових потоків до 10 Гбіт / с при показнику бітових помилок всього 10-12, що неможливо досягти при використанні будь-яких інших бездротових технологій;

- відсутня необхідність отримання дозволу на використання частотного діапазону. FSO-системи використовують інфрачервоний діапазон електромагнітного спектра далеко за кордоном 400 ГГц, тому ніяких ліцензій і спеціальних дозволів не потрібно;

- висока захищеність каналу від несанкціонованого доступу і скритність. Жодна бездротова технологія передачі не може запропонувати таку конфіденційність зв'язку як лазерна. Перехопити сигнал можна тільки встановивши сканери-приймачі безпосередньо в вузький промінь від передавачів. Реальна складність виконання цієї вимоги робить перехоплення практично неможливим. А відсутність яскраво виражених зовнішніх ознак (в основному, це електромагнітне випромінювання) дозволяє приховати не тільки передану інформацію, а й сам факт інформаційного обміну. Тому лазерні системи часто застосовуються для різноманітних додатків, де потрібна висока конфіденційність передачі даних, включаючи фінансові, медичні та військові організації;

- високий рівень завадостійкості і перешкодозахищеності. FSO- обладнання не сприйнятливе до радіоперешкод;

- можливість встановити лазерну атмосферну лінію там, де важко прокласти дротову лінію зв'язку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вишневський В., Кравець С., Шахновіч І. Енциклопедія WiMAX. Шлях до 4G. - М .: Техносфера, 2009. - 470 с. - ISBN 978-5-94836-223-6.

2. Вишневський В., Кузнецов С., Лаконцев Д., Поляков С. Гібридне обладнання на базі радіо - і лазерної технологій "Первая миля" 2007

УДК 004.7

Юлія Засіпко, студентка 172м-17-1
Науковий керівник: Галушко О.М., к.т.н., доц. кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ОПТИМІЗАЦІЯ МЕРЕЖІ WI-FI НАВЧАЛЬНОГО ПІДРОЗДІЛУ

Сфера застосування технології Wi-Fi досить широка. Можливо її як комерційне, так і домашнє використання. Зростає також необхідність використання мереж Wi-Fi в сфері медицини та освітніх установах. У навчальних закладах бездротовий доступ дозволяє підвищити рівень і якість навчання за умов широкого використання мобільних пристроїв. Wi-Fi дає миттєвий доступ до найбільш актуальної інформації з мережі Інтернет, будь-які довідкові посібники, бібліотеки. Тому важливо забезпечити якомога більше покриття бездротовою мережею не тільки навчальних приміщень, а й прилеглу територію, де це необхідно.

Важливо приділяти увагу плануванню та проектуванню Wi-Fi на етапі розгортання мережі або її оптимізації. Обов'язково потрібно знайти та передбачити всі нюанси, які можуть вплинути на якість роботи мережі в майбутньому. Сприяє в цьому радіо-обстеження на початковому етапі проектування бездротової мережі, що враховує план приміщення, проект установки точок доступу Wi-Fi, особливості поширення радіохвиль.[1]

Проведення вимірювань з реальним обладнанням, називається Site Survey. При цьому отримується реальна карта рівня сигналів площі від існуючих точок доступу Wi-Fi. За підсумками Site Survey, в разі знаходження діапазону з низьким рівнем сигналу, обладнання переміщують і знаходять найкраще положення, або збільшують кількість точок доступу. Таким чином, оптимізується рівномірність покриття приміщення та можливість надання якісного сервісу.

Зазвичай розробка стійкої мережі проводиться за допомогою програмного комплексу проектування бездротових мереж. Даний комплекс дозволяє змоделювати реальну ситуацію на об'єкті та розрахувати приблизну кількість обладнання, його карту розміщення і покриття, типи антен і багато інших параметрів. На підставі цих даних проводиться остаточний вибір обладнання та складання попередньої деталізації.[2]

Для роботи з бездротовими мережами існує достатня кількість багатофункціонального програмного забезпечення, що дозволяє здійснювати всебічне тестування Wi-Fi мереж. Такими програмами, наприклад, є: Ekahau Heat Mapper, NetSpot, Tamograph, Air Magnet Survey, Acrylic Wi-Fi Heatmaps, Visi Wave Site Survey.

Бездротова мережа Національного ТУ «Дніпровська політехніка» не є досконалою, тому вона потребує оптимізації. Отримання карти покриття частини приміщення від реального обладнання за допомогою програми NetSpot наведено на рисунку 1. Ідеальним Wi-Fi сигналом вважається рівень від -60 dBm до -65 dBm. Все що вище -60 dBm (наприклад -45 dBm) - це занадто потужний сигнал, все що нижче -80 dBm (наприклад -87 dBm) - слабкий сигнал. [3]

Результат планування представлений на рисунку 2, де проілюстровано значне поліпшення рівня сигналу, за допомогою переміщення обладнання.

Висновки: Wi-Fi - сучасна технологія, яка все сильніше впроваджується в багатьох сферах і знімає обмеження на переміщення користувача. Тестування Wi-Fi мереж та планування покриття за допомогою певного програмного забезпечення дозволяє досягнути якісного надання доступу до бездротової мережі та підвищити ефективність навчального процесу.

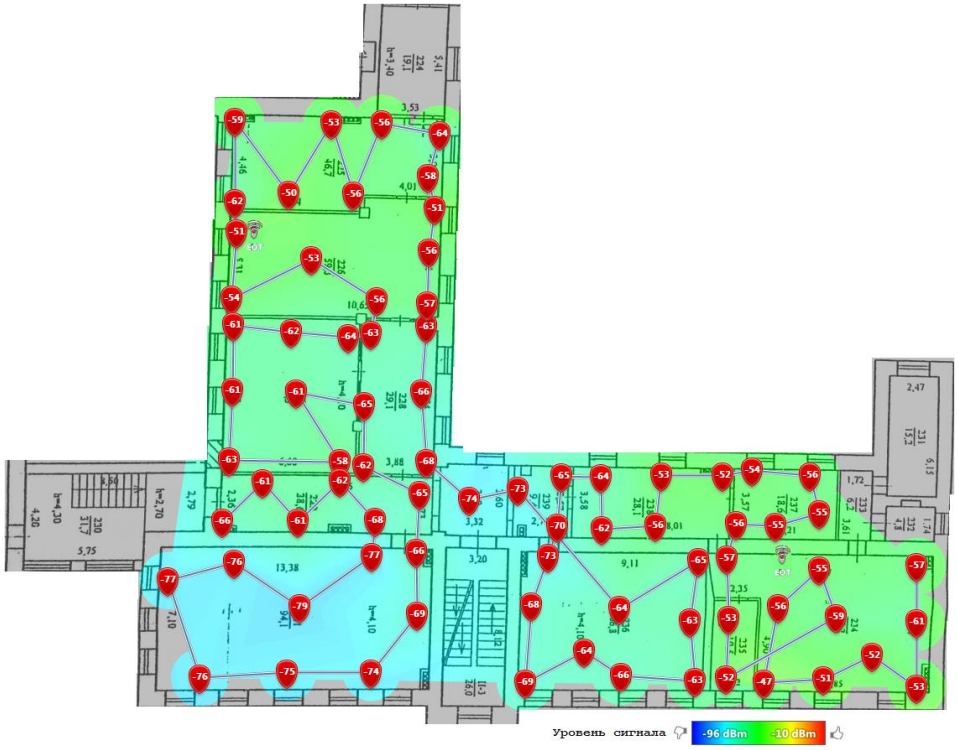


Рисунок 1 – Результат вимірювання рівня сигналу за допомогою NetSpot

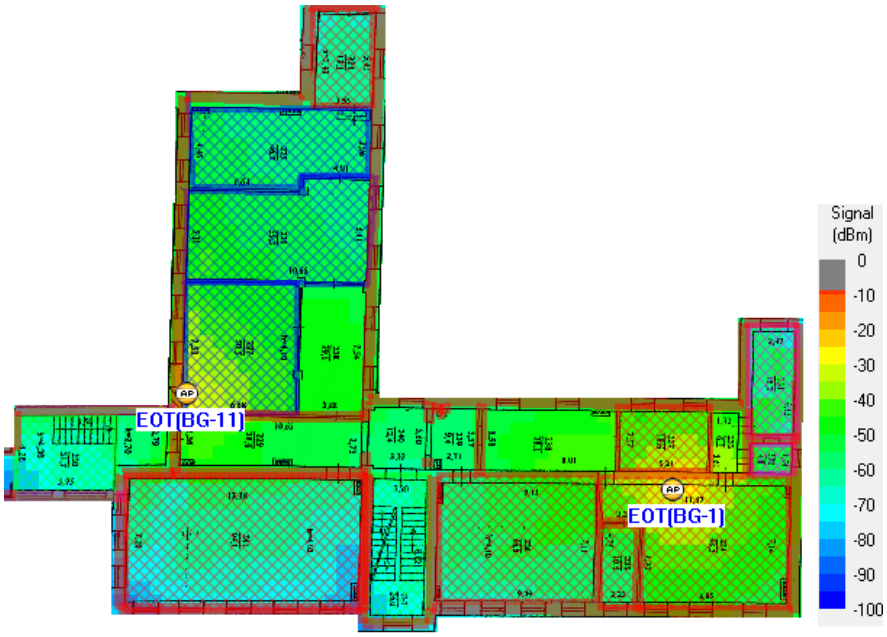


Рисунок 2 – Результат планування за допомогою AirMagnet Survey

ПЕРЕЛІК ПОСИЛАНЬ

1. Проектування Wi-Fi - прерогатива професіоналів [Електронний ресурс] https://www.2test.ru/publications/proektirovanie-wi-fi-prerogativa-professionalov.html
2. Проектування бездротових мереж [Електронний ресурс] https://www.lankey.ru/svyaz/network-solutions/wifi/proektirovanie/
3. Як посилити wifi сигнал [Електронний ресурс] http://www.linuxshop.ru/articles/a11761338-kak_usilit_wifi_signal

УДК 004

Талапова М.Д. студентка гр. 172м-17-1
Науковий керівник: Мєшков В.І., ст. викл. кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ВЗАЄМОЗВ'ЯЗОК АРХІТЕКТУРИ МЕРЕЖІ SDN ТА ПРОТОКОЛУ OPENFOW

В останні роки активно досліджуються питання інтеграцій різних видів послуг в мережах наступних поколінь (NGN) [1-3]. Значна частина інновацій в цьому напрямку орієнтовані на використанні вже адаптованих технологій, в тому числі – на основі поступового переходу від протоколу версії IPv4 на версію IPv6, який має розширене адресний простір і додаткові можливості управління потоками.

Такий підхід, можливо, є виправданим компромісом між існуючою інфраструктурою мережі Інтернет та новими викликами часу. Альтернативним варіантом реалізації транспортної функції в мережах NGN є концепція програмно-конфігуруються мереж (SDN), для яких ключовим елементом виступає протокол OpenFlow.

Загальна архітектура SDN показана на рис. 1.1. Вона складається з трьох рівнів: управління, інфраструктури і застосування [4-6]. «Інтелект» SDN мережі логічно зосереджений в програмованих SDN-контролерах, які забезпечують загальний моніторинг ресурсів мережі. Концепція SDN зміщує акцент з побудови розподіленої плоскої і однорівневої конфігурації (об'єднання мереж за типом «рівний з рівним») в бік переходу до ієрархічної централізованій архітектурі.

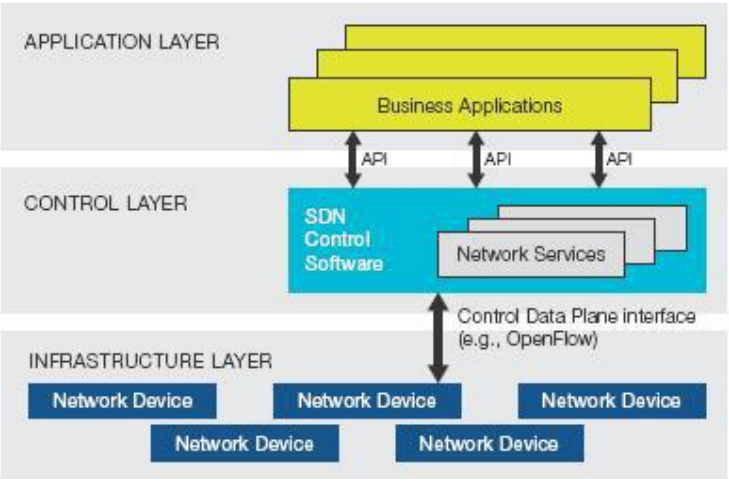


Рисунок 1.1. Узагальнена архітектура SDN

Передбачається, що централізоване планування і управління ресурсами SDN мережі відкриє нові можливості для оптимізації її функціонування та адаптації до постійно змінюваних умов (циклічні трендові флуктуації трафіку, випадкові пошкодження каналів або обладнання та ін.). Контролери підтримують кілька драйверів, які керують процесами підлеглих логічних елементів мережі, забезпечуючи, таким чином, надання необхідних мережевих послуг.

Контролер SDN забезпечує функціонування, продуктивність і управління обробкою несправностей в роботі по протоколу SNMP і іншим стандартним протоколам. Ця функція є, в певному сенсі, проміжним мережевим рівнем, який абстрагується від нижчих фізичних мережевих компонентів, таких як: комутатори, маршрутизатори, міжмережеві фільтри і диспетчери навантаження. В результаті, мережеві додатки представлені як цілісна система в вигляді єдиного логічного комутатора.

Використовуючи централізовані «інтелектуальні» SDN-контролери, можна змінити поведінку мережі в режимі реального часу і впровадити нові програми та послуги протягом декількох годин або днів, а не протягом тижнів і місяців, як це відбувається традиційно.

OpenFlow є першим стандартом інтерфейсу зв'язку між верхніми рівнями управління і пакетами підтримки SDN-рішень. Він реалізує переваги прямого доступу до мережевих пристроїв для управління і передачі даних, таких як комутатори і маршрутизатори (які визначені як фізичні або віртуальні сутності). Відсутність на ринку відкритих інтерфейсів для управління потоками даних робить сучасні мережеві пристрої замкнутими.

Як показано на рис. 1.2, протокол OpenFlow визначає основні примітиви, які можуть бути використані для зовнішнього програмного конфігурування мережевих пристроїв обробки даних, подібно до того, як програмний код реалізується центральним процесором в комп'ютерній системі. Він реалізується на обох кінцях інтерфейсу між пристроями та програмним забезпеченням менеджера мережевої інфраструктури SDN. Протокол використовує концепцію, яка полягає в ідентифікації потоків трафіку на основі заздалегідь визначених критеріїв, які можуть бути статично або динамічно запрограмовані головним пристроєм SDN.

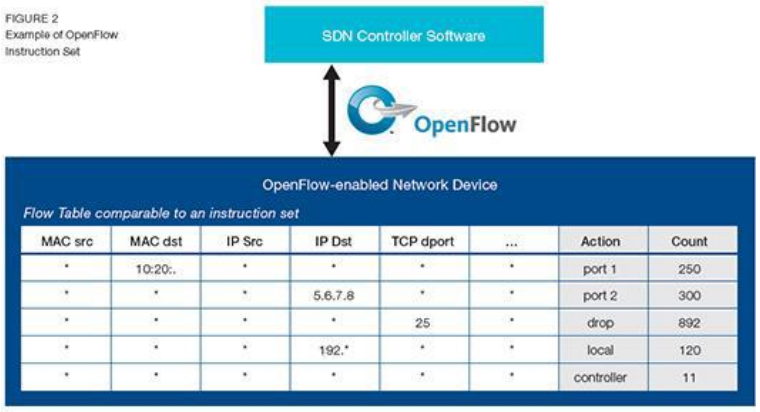


Рисунок 1.2. Приклад набору команд в таблиці OpenFlow

Протокол OpenFlow є ключовим компонентом для SDN, і на сьогоднішній день, він є поки єдиним стандартизованим протоколом, за допомогою якого можна безпосередньо контролювати площину мережевих пристроїв для просування пакетів. Мережі SDN з імплементацією протоколу OpenFlow можуть бути розгорнуті на існуючих мережах, як фізичних, так і віртуальних. При цьому мережеві пристрої можуть підтримувати як традиційні, так і орієнтовані на OpenFlow методи просування пакетів; це дозволяє корпораціям і провайдерам поступово впроваджувати SDN-технологію, навіть у разі використання мережевого обладнання різних виробників.

Комутатор OpenFlow об'єднує, як мінімум, три функціональних компонента. Перший компонент – це таблиця переходів з діями, які обумовлені дескрипторами потоків, що визначають способи обробки потоків комутаторами. Другий компонент - захищений канал, що з'єднує комутатор з віддаленим контролером, в якому пристрої обмінюються командами і пакетами. Третій компонент – це власне протокол OpenFlow, який підтримує обмін.

ПЕРЕЛІК ПОСИЛАНЬ

1. ITU-T Recommendation Y.2001 (12/2004). General overview of NGN. – Режим доступу: http://www.itu.int/rec/T-REC-Y.2001-200412-I/en.

2. Gilles Bertrand. The IP Multimedia Subsystem in Next Generation Networks / Gilles Bertrand. – 2007. – Режим доступу: http://www.rennes.enst-bretagne.fr/~gbertran/files/IMS_an_overview.pdf.

3. Yong Zheng. The Next Generation Network: Issues and Trends/Yong Zheng; Auckland University of Technology-2008-47 p.

4. SDN Basics – What You Need to Know about Software-Defined Networking. – Available at http://www.slideshare.net/SDNCentral/sdnu-101-final .

5. Тіхонов В.І. Метод динамічного управління цифровими потоками в інтегрованій технології телекомунікацій UA-ITT / В.І. Тіхонов // Наукові праці ОНАЗ ім. О.С.Попова. – 2013 р. – № 1. – С. 64-72.

6. SDN architecture. Issue 1, June, 2014, ONF TR-502. – Available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

УДК 004.7

Анна Норець, студентка 172м-17-1
Науковий керівник Корнієнко В.І., д.т.н., проф. кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ФІЛЬТРАЦІЯ ЗАШУМЛЕНИХ СИГНАЛІВ І ЗОБРАЖЕНЬ ІЗ ЗАСТОСУВАННЯМ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Цифрова фільтрація зашумлених сигналів і зображень важлива при вирішенні широкого кола науково-технічних завдань[1,2]. Такі завдання виникають, зокрема, в техніці зв'язку для поліпшення якості прийому переданих повідомлень. Традиційно, для очищення інформаційних повідомлень від перешкод застосовуються підходи, що використовують перетворення Фур'є. Але фільтри на основі перетворення Фур'є не дозволяють ефективно усувати ізольовані особливості сигналів, а також апарат перетворення Фур'є був розроблений для стаціонарних випадкових процесів, чиї характеристики незмінні в часі. Багато процесів у природі є нестаціонарними, і при їх обробці слід враховувати існуючі обмеження класичного спектрального аналізу. Цей фактор призвів до формування теорії вейвлет-аналізу, яка стала свого роду революцією в задачах цифрової обробки сигналів.

Застосування одномірного дискретного вейвлет-перетворення (1D-ДВП) є стандартним методом вейвлет-фільтрації сигналів, який до теперішнього часу детально вивчений і широко застосовується в багатьох областях науки і техніки.

Застосування ДВП для цифрової фільтрації сигналів і зображень є більш перспективним підходом в порівнянні з перетворенням Фур'є через можливість ефективного усунення локалізованих перешкод. ДВП, зазвичай використовується в рамках багатомасштабного аналізу, здійснює розкладання сигналу або зображення на складові, які відносяться до різних масштабів спостереження. Так, формат представлення графічних даних JPEG2000 передбачає застосування ДВП з ортонормованими базисами і обнулення малих вейвлет-коефіцієнтів. При аналізі зашумлених зображень це забезпечує одночасну фільтрацію перешкод і зменшення розміру зображення, а відсоток стиснення файлів характеризує відносне число похилої вейвлет-коефіцієнтів. Аналогічна ідеологія використовується у форматах цифрового відео (MPEG) і графічних файлів (DJVU).

Зазначимо, що при вирішенні подібного роду завдань простий варіант обнулення частини вейвлет-коефіцієнтів може бути недостатньо ефективним, приводячи до спотворень відновленого сигналу або зображення. У науковій літературі обговорюються варіанти різної корекції вейвлет-коефіцієнтів, включаючи способи "жорсткого" і "м'якого" завдання порогової функції в просторі вейвлет-коефіцієнтів. Жорсткий варіант передбачає вибір порогового значення і обнулення тільки тих коефіцієнтів розкладання, які не перевищують по модулю порогове значення. Головним недоліком жорсткого варіанта завдання порогової функції є існування розривів, що призводять до порушення регулярності сигналу на етапі його синтезу. Однак при цьому великі коефіцієнти не змінюються, і проведена фільтрація не призводить до зміни амплітуди відновленого сигналу.

М'який варіант завдання порогової функції дозволяє уникнути розривів, але передбачає коригування всіх коефіцієнтів. Це дозволяє знизити ефект порушення регулярності сигналу, але впливає на його амплітудні характеристики. Проте, у багатьох завданнях, що відносяться до передачі інформації, остання обставина не є критичною. З цієї причини підвищення якості очищення сигналів від перешкод є більш важливою обставиною, ніж збереження незмінною амплітуди сигналу.

М’який варіант фільтрації на основі ДВП є стандартним методом, широко застосовуваним на практиці. Однак він теж має ряд недоліків: осциляції вейвлет-коефіцієнтів в околиці сингулярностей, що ускладнюють обробку сигналів, відсутність інваріантності відносно зсуву, поява артефактів в реконструйованому сигналі після корекції вейвлет-

коефіцієнтів. З метою усунення цих недоліків у роботах був запропонований метод дуального комплексного вейвлет-перетворення.

Метод ДКВП передбачає незалежне обчислення двох ДВП, в результаті яких визначаються дійсні і уявні частини вейвлет-коефіцієнтів. Проведені до цього часу дослідження підтвердили, що цей метод є корисною модернізацією ДВП[3]. Він зберігає всі переваги, але додатково дозволяє оперувати з амплітудами і фазами вейвлет-коефіцієнтів, розширюючи можливості аналізу експериментальних даних. Для забезпечення вимоги аналітичних базисних функцій в рамках ДКВП застосовують спеціальні прийоми побудови базисів.

Виконавши порівняльний аналіз різних прийомів фільтрації, було з'ясовано наступне:

- для підвищення якості вейвлет-фільтрації та зменшення ймовірності внесення випадкових спотворень при реконструкції сигналу доцільно використовувати безперервні і гладкі порогові функції на етапі корекції коефіцієнтів вейвлет-перетворення;
- фільтрація зашумлених сигналів і зображень на основі дуального комплексного вейвлет-перетворення забезпечує зниження середньоквадратичної помилки відновлення сигналу по вейвлет-коефіцієнтів у порівнянні з фільтрами на основі дискретного вейвлет-перетворення, використовує базиси вейвлетів Добеші;
- при фільтрації аудіо-сигналів, що містять мовні повідомлення, комплексне вейвлет-перетворення подвійної щільності дозволяє обмежитися меншим числом рівнів розкладання сигналу в базисі вейвлет-функцій у порівнянні з фільтрами на основі вейвлетів Добеші, щоб досягти максимальне значення середньої оцінки розбірливості мови.

Отже, незважаючи на розвиток прийомів цифрової фільтрації, що використовують вейвлет-перетворення, при практичному застосуванні даних методів зберігається багато відкритих питань, і вибір конкретного способу фільтрації залишається нетривіальним завданням, багато в чому залежить від аналізованого сигналу і цілей, які потрібно досягти в ході цифрової обробки експериментальних даних.

ПЕРЕЛІК ПОСИЛАНЬ

[1] Оппенгейм, А. Цифровая обработка сигналов / А. Оппенгейм, Р. Шафер. – М.: Техносфера, 2007.

[2] Каплан, Д. Практические основы аналоговых и цифровых схем / Д. Каплан, К. Уайт. – М.: Техносфера, 2007.

[3] Belzer, B. Complex, linear-phase filters for efficient image coding / B. Belzer, J. M. Lina, J. Villasenor // IEEE Trans. Signal Processing. – 1995. – Vol. 43(10). – P. 2425-2427.

УДК 004.7

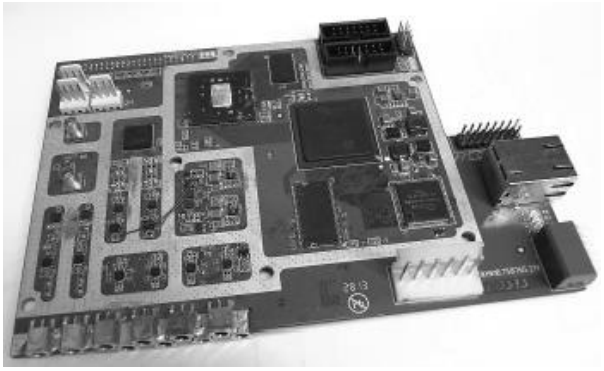
Олексій Марков, студент 172м-17-1
Науковий керівник: Герасіна О.В., к.т.н., доц. кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

ПРИСТРІЙ ФОРМУВАННЯ ВУЗЬКОСМУГОВИХ РАДІОСИГНАЛІВ З ВИКОРИСТАННЯМ АЛГОРИТМУ ОПТИМАЛЬНОЇ ІНТЕПРОЛЯЦІЇ

Нині йде активне впровадження мереж 4-го покоління мобільного зв'язку (технологія LTE) і систем цифрового телебачення (технологія DVB - T2), розвиток систем глобального позиціонування, широко використовуються мобільні мережі 2-го і 3-го покоління (технології GSM і 3g), системи безпровідної передачі інформації в локальних мережах (технологія WLAN) і інші.

Приймально-передавальні пристрої кожної системи проходять цикли розробки, виробництва і експлуатації, і на кожному етапі необхідно контролювати безліч параметрів. Для цього створюються спеціалізовані вимірювальні пристрої. До подібних пристроїв відноситься генератор векторних сигналів універсальний прилад, призначений для формування точних і спотворених вузькосмугових радіосигналів. Вітчизняні аналоги такого пристрою відсутні або не мають необхідних функціональних можливостей, що підтверджує актуальність розробки власної продукції. Аналіз показує, що більшість радіосистем передачі інформації працюють в діапазоні частот від 54 Мгц (технологія WLAN, стандарт IEEE 802.11af) до 5875 Мгц (технологія WHDI) із смугою сигналу від 10 кГц (технологія Tetrapol) до 160 Мгц (технологія WLAN, стандарт IEEE 802.11ac). Тому генератор векторних сигналів має бути широкосмуговим пристроєм, здатним формувати достовірно точні вузькосмугові сигнали.

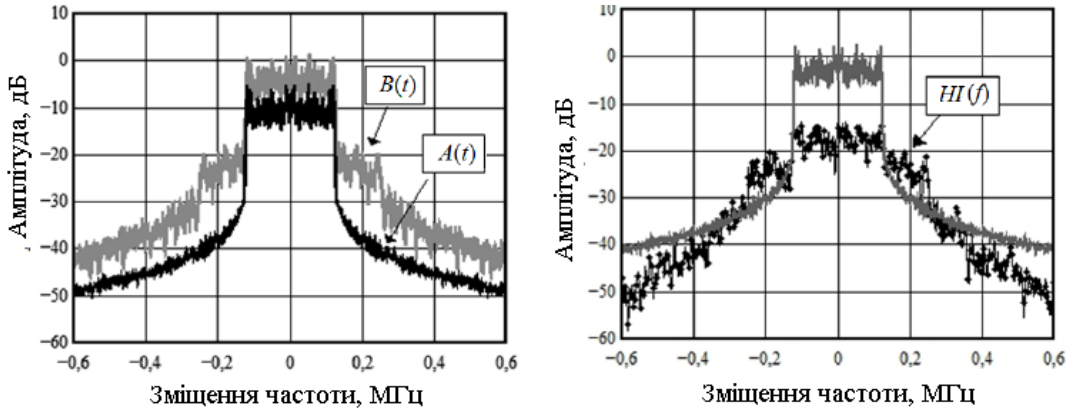
Для тестування вимірювального комплексу використовувався вузькосмуговий радіосигнал з модуляцією QAM16, що займає смугу в 250 кГц на частоті сигналу, що несе, рівній 3 ГГц. Досліджуваним пристроєм виступав підсилювач. Сигнал до і після (B (t)) досліджуваного пристрою оцифровується за допомогою векторного аналізатора ланцюгів.



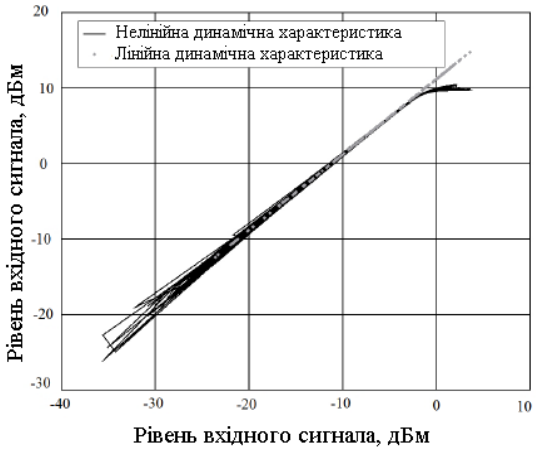
Дослідний зразок плати універсального генератора модулюючих сигналів

У розробленому пристрої використовується ПЛІС фірми Xilinx Inc. серії Kintex XC7K70t. Вона містить 10250 логічних секцій, кожна з яких складається з чотирьох шестивходовых таблиць перетворення і восьми тригерів, а також двісті сорок секцій ЦОС . Кількість ресурсів достатня для реалізації системи підвищення частоти дискретизації (таблиця 3.2), а також систем формування і корекції сигналів. Приведені в таблиці дані отримані в програмному забезпеченні Vivado Design Suite після розміщення системи підвищення частоти дискретизації на кристалі. При розрахунку загальної кількості ресурсів враховувалося, що система використовуватиметься для формування синфазної і квадратурної складових сигналу.

Для кожного з каналів використовуються свої що коригує і інтерполяційний фільтри, а усі інші блоки загальні.



Амплітудно-частотні характеристики виміряних (а) і розрахованих (б) сигналів



Динамічні характеристики досліджуваного пристрою

ПЕРЕЛІК ПОСИЛАНЬ

1. Абраменко А.Ю. Структура універсального генератора сигналів / А.Ю. Абраменко, Г.Г. Гошин // Доповіді ТУСУР. - 2013. - № 3 (29). - С. 5-9.

2. Голденберг Л.М. та ін. Цифрова обробка сигналів: Учеб. Посібник для вузів / Голденберг Л.М., Матюшкін Б.Д., Поляк М.Н. - 2-е изд., Перераб. і доп. - М.: Радио и связь, 1990. - 256 с.

3. Баскаков С.І. Радіотехнічні ланцюги і сигнали: Підручник для вузів / 2-е вид., Перераб. і доп. - М .: Вища школа, 1988. - 448с.

4. Абраменко А.Ю. Дослідження алгоритму оптимальної інтерполяції і його апаратно-програмна реалізація на ПЛІС // Електронні засоби та системи управління: матеріали доповідей міжнародної науково-технічної конференції. - 2012. - Ч. 1. - С. 9-1

УДК 621.39

Аліна Сімонова, студентка 172м-17-1
Науковий керівник: Галушко О.М., к.т.н., доц. кафедри БІТ
Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

УДОСКОНАЛЕННЯ МОДЕЛІ РОЗПОВСЮДЖЕННЯ РАДІОХВИЛЬ В УМОВАХ ЩІЛЬНОЇ ЗАБУДОВИ МІКРОРАЙОНІВ МІСТА

Сучасні міські райони характеризуються щільною забудовою місцевості будівлями і спорудами, що є причиною швидких завмирань радіосигналу в каналі зв'язку. Радіотраси з точки зору поширення радіохвиль являють собою складну структуру, так що опис їх практично є неможливим без спрощень, які визначаються для конкретних умов розповсюдження радіохвиль.

В умовах міської забудови загасання радіосигналу є випадковою величиною і залежить від комплексу факторів, що визначають характер поширення радіохвиль [1]. Причинами втрат рівня сигналу стільникового зв'язку є наступні фактори:

• відображення сигналу від об'єктів, що мають розміри, що перевершують довжину радіохвилі;

• дифракція радіохвиль, для якої характерно переломлення радіосигналу на шляху поширення;

• розсіювання радіосигналу, яке відбувається при наявності на місцевості великого числа об'єктів, розміром менше довжини радіохвилі (наприклад, листяні дерева);

• ефект Допплера, що має місце при переміщенні рухомого об'єкту.

Моделі прогнозування втрат сигналу на трасі умовно поділяються на два типи: емпіричні та теоретичні. Емпіричні моделі зазвичай представляють собою набір рівнянь, отриманих в результаті значних польових вимірювань.

Емпіричні моделі є простими і ефективними у використанні, проте вони точні для середовищ з характеристиками, ідентичними характеристиками середовищ, де проводилися вимірювання. Вхідні параметри для емпіричних моделей, як правило, якісні і не дуже конкретні, наприклад, щільна міська площа, сільська місцевість, і так далі. Одним з головних недоліків емпіричних моделей є те, що вони не можуть бути використані для різних середовищ без змін, а іноді вони просто не приносять користі.

Ослаблення сигналу розглянемо за допомогою емпіричної моделі COST 231- Хата для міста Дніпро, мікрорайону Лівобережний 3.

Однотипний за характером забудови міській район без великих площ і парків, в якому на 1 кв.км. в середньому припадає до 70-ти 9-ти та 10-ти поверхових будівель. Середня довжина будівель 60 - 80 м, ширина 10 - 15 м.

Система зв'язку - система стільникового зв'язку стандарту GSM900, GSM1800. Тип антени - панельна. Висота установки 30 - 40 м.

Модель Хата виникла в результаті адаптації емпіричних формул з графіками, складеними Окамура з співавторами на основі результатів польових випробувань.

Модель Хата широко використовується в різних країнах. Вона в якості основи розглядає міські райони.

Розрахунки втрат по трасі поширення радіосигналу найчастіше в даний час проводять за допомогою моделі COST 231 Хата. Умови застосовності моделі: f = 1500-2000 МГц; $H_{БС}$ = 30 -200 м; $H_{АС}$ = 1-10 м., R - має бути між 1 км та 20 км. [2].

Середнє загасання радіосигналу в міських умовах розраховується за наступною емпіричною формулою.

$$L_M = 48,55 + 35,4lgf - 13,82lgH_{БС} – (1,1lgf – 0,7)H_{АС} +(44,9 - 6,55lgH_{БС})lgR, \text{ дБ}$$

де: $H_{БС}$ - ефективна висота підйому антени базової станції, м; $H_{АС}$ - висота антени мобільної станції над землею, м; R - відстань між передавачем і приймачем, км; F - частота сигналу, МГц;

Отже, при досить щільній забудові, відповідність реальних значень потужності сигналу в точці прийому при відстані менш 1 км значно відрізняється від отриманих за наведеною моделлю. Треба також відмітити, що сучасні мережі стільникового зв'язку набагато більш базових станцій на одиницю площі, ніж це визначається теорією планування мобільних мереж. Це пов'язано з значно більшим трафіком і не стільки речовим, а також і мобільного Інтернету. В цих умовах визначення реальних значень потужностей сигналів в точках прийому становить ще важливішим.

Метою проведеного дослідження й стало визначення параметрів розповсюдження для удосконалення моделей, в особистості моделі COST 231- Хата при відстані між АС та БС менш 1 км.

Результати вимірювань, та статистична обробка наведені на рисунку 1.

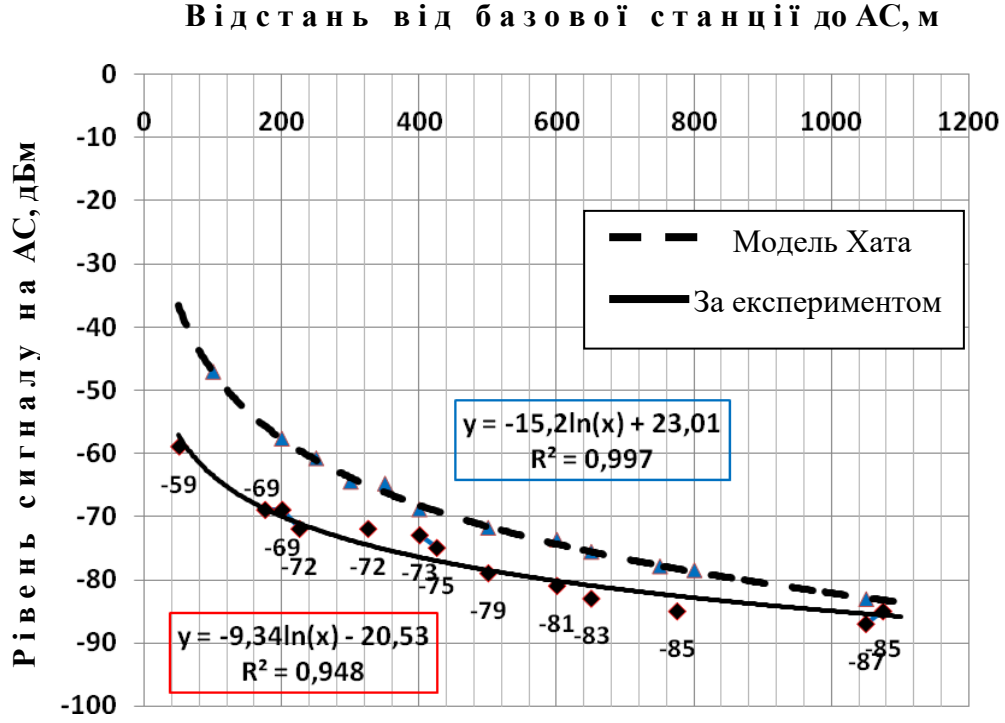


Рисунок 1 – Результати вимірювань рівню сигналів на АС та їх визначення за моделлю COST 231- Хата.

З отриманих результатів можна зробити висновок про необхідність удосконалення моделі (в особистості COST 231- Хата) для відстаней між АС та БС менш 1 км., а також і для різних типів забудов як етажності будівель, так і щільності їх розташування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Гавриленко В.Г., Яшнов В.А. Распространение радиоволн в современных системах мобильной связи. Нижний Новгород 2003, 148 с.

2. Колодезная Г.В. Основы теории связи с подвижными объектами. Методическое пособие по курсовому проектированию. Хабаровск, Издательство. ДВГУПС, 2012, 26 с.

X ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

22 листопада 2018 р.

Підписано до друку 20.11.18. Формат А4.
Ум. друк. арк. 7,4. Обл.-вид. арк. 7,2. Елект. видання.

Підготовлено у НТУ «Дніпровська політехніка»
49005, м. Дніпро, просп. Д. Яворницького, 19