ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ім. Г.Є. ПУХОВА
УНІВЕРСИТЕТ В БЄЛЬСЬКО-БЯЛІЙ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
ДНУ «ІНСТИТУТ ОСВІТНЬОЇ АНАЛІТИКИ» МОН УКРАЇНИ
РЕДАКЦІЯ НАУКОВИХ ЖУРНАЛІВ
«БЕЗПЕКА ІНФОРМАЦІЇ» І «ЗАХИСТ ІНФОРМАЦІЇ»
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

SIST-2021

ЗБІРНИК ТЕЗ НАУКОВИХ ДОПОВІДЕЙ

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ
ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

23 – 26 червня 2021 року
МИКОЛАЇВ – КОБЛЕВО

Збірник тез наукових доповідей. Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2021) – Миколаїв - Коблево: 2021. – 78 с.

У збірник ввійшли матеріали, представлені і обговорені під час проведення 13-ої Всеукраїнської науково-практичної конференції «**СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО–ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (SITS' 2021)**» 24-26 червня 2021 року в с. Коблево Миколаївської області.

Матеріали збірника можуть бути корисними для науковців і фахівців сфер інформаційних технологій та кібербезпеки, менеджменту персоналом підприємств і установ, професорсько-викладацького складу закладів вищої освіти, аспірантів і студентів.

Матеріали публікуються за оригіналами, наданими авторами.

МИКОЛАЇВ – КОБЛЕВО
2021

ЗМІСТ

НЕЙРОМЕРЕЖЕВА СИСТЕМА РОЗПІЗНАВАННЯ ПОЛІМОРФНИХ КОМП'ЮТЕРНИХ ВІРУСІВ

Погорелов В.В., Коломієць М.В., Бичков В.В.
Національний авіаційний університет

В теперішній час системи антивірусного захисту (САЗ) є одним з основних засобів захисту інформації більшості комп'ютерних систем і мереж. Не зважаючи на те, що такі системи використовуються вже не одне десятиліття і їх розробкою та створенням методологічної бази займаються висококваліфіковані фахівці, практичний досвід і результати багатьох науково-практичних досліджень вказують на наявність суттєвих недоліків в сучасних антивірусах. Основним з яких є недостатня точність розпізнавання всієї номенклатури комп'ютерних вірусів [1] та висока похибка розпізнавання поліморфних комп'ютерних вірусів, що підтверджується відомими випадками успішних вірусних кібератак на вітчизняні та закордонні комп'ютерні системи і мережі. Однак впровадження відомих засобів розпізнавання комп'ютерних вірусів у вітчизняні системи захисту інформації викликає необхідність їх складної адаптації до очікуваних умов використання. Також недоліками відомих засобів розпізнавання є висока вартість і відсутність докладної науково-технічної документації.

Важливим напрямком підвищення точності розпізнавання є «інтелектуалізація» методів розпізнавання за рахунок використання теорії штучних нейронних мереж (НМ). Перспективність вказаного напрямку підтверджується окремими вдалими застосуваннями НМ в засобах розпізнавання комп'ютерних вірусів (антивірус з відкритим програмним кодом ClamAV, стартап Deep Instinct) та великою кількістю відповідних теоретико-практичних робіт [2-5].

Разом з тим, недостатня точність розпізнавання та недостатня адаптованість до умов експлуатації, закритість використаних рішень, значно обмежують сферу їх застосування. При цьому постійний прогрес в області теорії НМ вказує на можливість значного вдосконалення апробованих засобів розпізнавання [6-8].

Дослідження вітчизняних та зарубіжних вчених, зокрема И. Бенджио (Yoshua Bengio), Бодянського Є. В., Я. Лекуна (Yann LeCun), Різника О.М., Руденка О.Г., Д. Хінтона (Geoffrey Hinton), З. Хохрайтера (Sepp Hochreiter) вказують на те, що перспективним шляхом підвищення ефекивності антивірусного захисту є застосування апарату НМ для розпізнавання комп'ютерних вірусів. Це пояснюється тим, що задача розпізнавання комп'ютерних вірусів є однією із основних при розробці САЗ, що підтверджується ефективністю використання НМ для вирішення подібних задач оцінки параметрів безпеки інформаційних систем у відомих засобах захисту інформації (AVZ, продукція компаній Cisco, Symantec) та є доведеною адаптивністю нейромережевих засобів (НМЗ) розпізнавання до умов застосування в САЗ.

В такій постановці проблеми є актуальною науково-прикладна задача розробки ефективної нейромережевої системи розпізнавання поліморфних комп'ютерних вірусів, адаптованих до умов вітчизняних систем антивірусного захисту.

Для часткового вирішення вищезгаданих проблем розроблено експериментальну установку — нейромережеву систему розпізнавання поліморфних комп'ютерних вірусів.

Основною частиною установки став створений за допомогою мови Python кросплатформуний програмний додаток «DNN analyzer», що дозволяє реалізувати ГНМ. В процесі розробки комплексу використана загальнодоступна бібліотека TensorFlow (розробка компанії Google) призначена для моделювання ГНМ. Головне вікно додатку показане на рис. 1.

Управляючі елементи головного вікна розділені на три секції Database, DNN та Classification в котрих розміщені відповідні управляючі елементи (кнопки). Означені елементи інтерфейсу мають наступне призначення:

- Секція Database – вибір навчальної бази даних.

- Кнопка «Labeled Database» – ініціює режим вибору навчальної бази даних, що містить марковані приклади.

- Кнопка «Unmarked Database» – ініціює режим вибору навчальної бази даних, що містить не марковані приклади.

- Секція DNN – співвідноситься з реалізацією ГНМ.

- Кнопка «The choice of the type of DNN» - дозволяє обрати тип ГНМ.

- Кнопка «Set DNN parameters» - ініціює вибір архітектурних параметрів ГНМ.

- Кнопка «DNN training» - ініціює вибір параметрів навчання та запускає процес навчання ГНМ.

- Секція Classification - співвідноситься з застосуванням ГНМ для розпізнавання комп'ютерних вірусів.

- Кнопка «Specify recognition target» - ініціює режим вибору об’єктів, що підлягають розпізнаванню.

- Кнопка «Recognize» - запускає процес розпізнавання.

Використання програмного додатку «DNN analyzer» зводиться до послідовного застосування описаних елементів управління для вибору навчальної бази даних, вибору типу та задання архітектурних параметрів ГНМ, задання параметрів та реалізації навчання, вибору об'єкту, що має бути розпізнаний та власне реалізації процесу розпізнавання.

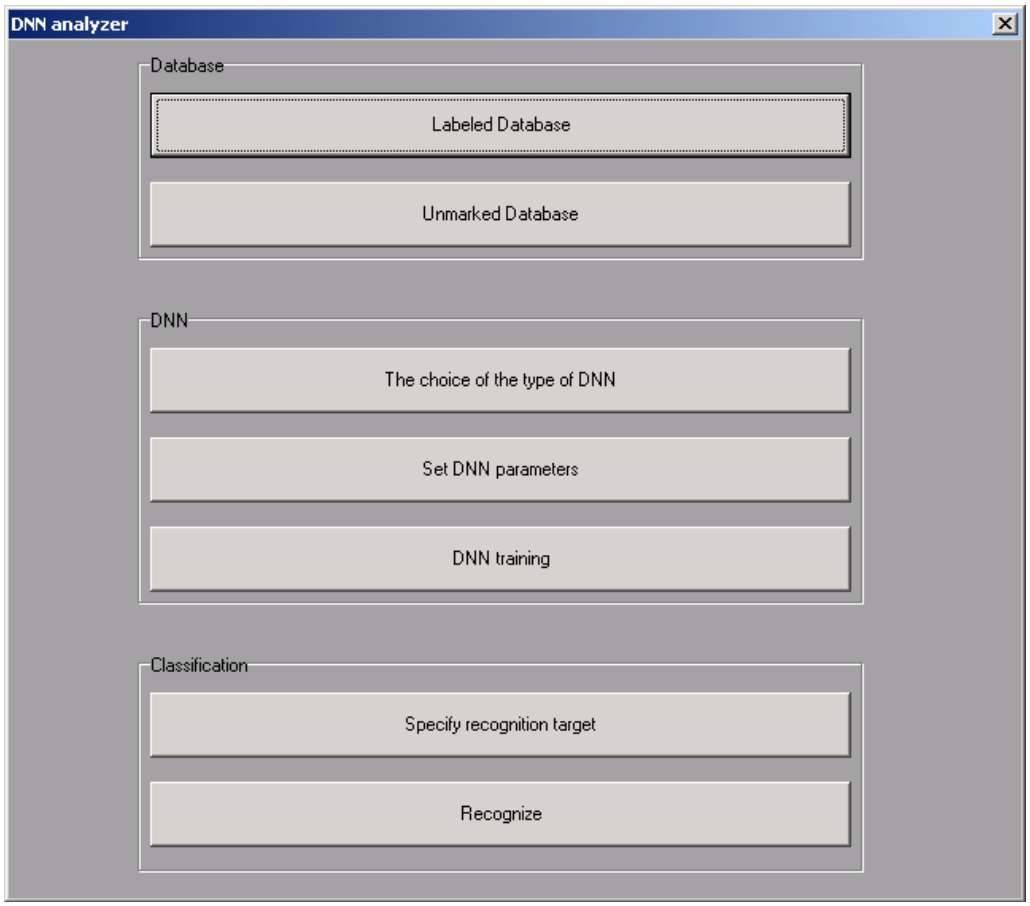


Рис. 1. Головне вікно додатку «DNN analyzer»

Особливості реалізації програмного додатку «DNN analyzer» полягали в застосуванні процедури онлайн навчання ГНМ та процедури формування вхідного шару ГНМ [5]. Процедура онлайн навчання — спрощена. Спрощення полягає у відсутності у схемі навчання елементів, що відповідають за часові обмеження процесу тренування та за особливості розділення навчальної вибірки на окремі блоки.

Висновки. Дана робота присвячена вирішенню науково-практичної задачі розробки нейромережевої системи розпізнавання поліморфних комп'ютерних вірусів. Експериментальна установка забезпечує можливість проведення експериментів, які показують, що при очікуваних умовах застосування розроблена нейромережева система дозволить забезпечити помилку розпізнавання поліморфних комп'ютерних вірусів в межах 0,03 - 0,05, що знаходиться на рівні кращих систем аналогічного призначення.

СПИСОК ЛІТЕРАТУРИ

1. I. Dychka, D. Chernyshev, I. Tereikovskyi, L. Tereikovska , V. Pogorelov, «Malware Detection Using Artificial Neural Networks», *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing*, Vol. 938. Springer, Cham, pp.3-12, 2019. (SCOPUS) DOI: *https://doi.org/10.1007/978-3-030-16621-2_1*.
2. I. Tereikovskyi, V. Pogorelov, O. Tereikovskyi, «Determination of structural parameters of a multilayer cyber threat detection perceptron», *Aviation in the XXI-st Century,* 2018, pp. 3.3.1 – 3.3.4.
3. І. Терейковський «Нейромережевий поведінковий аналізатор антивірусної системи», *Захист інформації*, № 2, С. 67-70, 2012.
4. І. Терейковський, «Нейронні мережі в засобах захисту комп’ютерної інформації: монографія», *К.: ПоліграфКонсалтинг*, 2007, 209 с.
5. І. Терейковський «Вдосконалення алгоритму навчання багатошарового персептрону, призначеного для розпізнавання мережевих атак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, Випуск 2(24), С. 65-70, 2012.
6. І. Терейковський, «Використання нейронних мереж при розпізнаванні макровірусів», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, Випуск 2 (13), С. 176-183, 2006.
7. І. Терейковський, «Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення», *Безпека інформації*, Т. 19, № 1,С. 24-28, 2013.
8. І. Терейковський, «Нейромережеві моделі, методи і засоби оцінювання параметрів безпеки інтернет-орієнтованих інформаційних систем», *Дисертація д-ра техн. наук: 05.13.21, Нац. авіац. ун-т.*, Київ, 2015, 430 с.

МЕТОД КЛАСТЕРИЗАЦІЙ, ЯК ГОЛОВНИЙ НАПРЯМОК ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЦОД

Шестак Я., Панасюк О, Торчило А., Огбу Д.
Київський національний університет імені Тараса Шевченка

При розробці методів забезпечення захисту ЦОД від кібератак крім побудови алгоритмів, що безпосередньо протидіють впровадженню шкідливого програмного забезпечення (ПО), важливо розглянути оптимізацію самої роботи інфраструктури ЦОД та запропонувати механізми прозорого виконання операцій і надійного збереження даних.

Базовими методами оптимізації роботи ЦОД є паралелізація та кластеризація, що відносяться як до розподілу апаратних ресурсів інфраструктури, так і до розподілу та планування списку завдань.

Кластеризація є методом аналізу даних ЦОД, в результаті котрого подібні інформаційні елементи аналогічно до елементів апаратних ресурсів об’єднуються у групи, що називаються кластерами. Кластеризація надає широкі можливості для забезпечення захисту інфраструктури ЦОД від кібератак, при цьому методологія захисту базується на наступних механізмах:

- організація прозорої схеми функціонування ЦОД;
- вивільнення апаратних ресурсів ЦОД;
- організація алгоритмів захисту ЦОД, що базуються на методі кластеризації.

Організація прозорої схеми функціонування ЦОД та вивільнення апаратних ресурсів ЦОД є непрямими засобами захисту ЦОД від кібератак. Прозора схема функціонування дозволяє виявити приховані канали, а збільшення ефективності роботи інфраструктури комплексу ВМ звільняє частину апаратних ресурсів ЦОД, що використовуються для виявлення та знешкодження кібератак.

Побудуємо схему виявлення кіберзагрози за рахунок наявних ресурсів ЦОД (рис. 1). Детектування потенційної загрози поділяється на детектування внутрішньої загрози та виявлення аномалій, що надходять зовні. У свою чергу, серед аномалій (потенційно небезпечного програмного коду) нас цікавлять ті, що надходять з мережі. Основна частина кібератак відслідковується методами активного моніторингу. Кластеризація використовується при пасивному моніторингу, зокрема, при глибинному аналізі коду.

Рис. 1. Детектування потенційної загрози сервісом ЦОД

Відстань між елементами, визначення якої є першим етапом кластеризації даних, визначається за допомогою відповідних систем оцінки. У основі метрики лежать d параметрів двох інформаційних елементів $x_i = (x_{i1} \dots x_{id})$ і $x_j = (x_{j1} \dots x_{jd})$, відстань між якими визначається як функція D_{ij} за одним з алгоритмів, що наведено у табл. 1.

Таблиця. 1

Методи визначення відстані при кластеризації відповідно до метрики

Метрика	**Визначення відстані**	**Позначення**
Мінсковського	$D_{ij} = \left[\sum_{i=1}^{d} \lvert x_{il} - x_{jl} \rvert^{\frac{1}{n}}\right]^{n}$	$n \in N$
Евклідова	$D_{ij} = \left[\sum_{i=1}^{d} \lvert x_{il} - x_{jl} \rvert^{\frac{1}{2}}\right]^{2}$	—

Манхеттенська	$D_{ij} = \sum_{i=1}^{d} \lvert x_{il} - x_{jl} \rvert$	—
Махаланобіса	$D_{ij} = (x_i - x_j)^T S^{-1} \cdot (x_i - x_j)$	T - транспонування S – коваріаційна матриця кластеру

Існує п’ять груп методів кластеризації даних:

1. **Ієрархічна кластеризація**, що також називається кластеризацією зв’язності, є класичним підходом узагальнення великих масивів даних. Даний метод створює кластери у вигляді деревоподібної структури, у якій кожний кластер представлений у вигляді вузла. При цьому дані кластеризуються відповідно до параметра подібності, і це стосується як елементів у кластері, так і груп кластерів. Алгоритми ієрархічного кластеризації, можуть бути сформовані за алгоритмом «знизу-вгору» і «згори-донизу».

Методи ієрархічної кластеризації дозволяють провести процеси ідентифікації та класифікації засобів наявних кібератак, передбачити вдосконалення алгоритмів кібератаки на основі цього, при цьому архітектура є достатньо гнучкою, що надає можливість масштабування системи під нові задачі.

Дана група методів є найбільш ефективною при роботі з DoS- та DDoS-атаками, так, наприклад алгоритми низькоенергетичної адаптивної кластерної ієрархії для забезпечення аналізу трафіку в кластері виявляє скомпрометованих вузли мережі та надсилає попередження функціональним вузлам кластерів. Інший підхід у даній сфері полягає у виявленні різких змін трафіку в декількох мережевих доменах. Така система захисту на рівні апаратних ресурсів має відслідковувати всі маршрутизатори, через які у паралельному режимі здійснюються кібератаки, що ускладнює її побудову, але суттєво збільшує ефективність.

2. У групі **методів часткової кластеризації масивів** розподіл даних відбувається за схемою k розділів і по n об’єктів за допомогою заданої цільової функції. Цільова функція при цьому визначається у відповідності до обраної метрики D_{ij}:

$$F_{ij} = \sum_{i=1}^{k} \sum_{j=1}^{n} D\left(x_j, c(i)\right), \quad (3)$$

де $c(i)$ — середнє значення кластеру.

У алгоритмах такого роду можна перемістити об'єкт з одного кластеру в інший кластер, щоб поліпшити якість кластеризації, що неможливо для ієрархічних алгоритмів.

Для виявлення атак найбільш ефективною показала себе гібридна система, яка поєднує часткову кластеризацію та наївний баєсівський класифікатор. Даний метод виділяє важливі атрибути програмного коду, що потенційно свідчать про наявність небезпечного коду та вилучає атрибути, що не актуальні, тобто виділяє непрогнозовану частину сигналу. Система виявляє вторгнення та далі класифікує його відповідно до базових категорій.

3. У алгоритмах **щільнісної кластеризації** кластери створюються на базі областей з високою концентрацією інформаційних об’єктів у відповідності до заданого порогового значення. Частина масиву, що залишилася, сприймається як шум і не аналізується. Таким чином усувається помилкове спрацьовування системи захисту.

4. **Ґратчаста кластеризація** базується на створенні кінцевого числа комірок шляхом квантування масиву даних та побудови структури сітки. Ця група методів залежить від кількості комірок, а не від кількості об'єктів, тому час їх обробки може бути меншим ніж для інших методів аналогічної складності. Базова схема такого методу кластерізації полягає у виконанні наступних етапів:

1) розбиття масиву даних на кінцеве число комірок, що не перекриваються;
2) розрахунок щільності кожної з комірок;
3) сортування комірок за їх щільністю;

4) визначення кластерних центрів;
5) відслідковування сусідніх комірок.

5. **Група методів кластеризації, що базуються на статистичних моделях,** включає у себе методи, що найбільшою мірою відрізняються між собою. Типовим підходом є визначення нормального профілю роботи мережі та виявлення аномалій, як критерію кібератаки. При цьому, з одного боку слід виявляти типові ознаки зараженої мережі, а з іншого — орієнтуватися на збільшення потоку передачі даних, що є характерним для роботи прихованого каналу.

Висновки. Кластеризація - один з основних напрямків оптимізації роботи ЦОД. Даний метод надає можливість суттєво спростити процес розробки алгоритмів кіберзахисту ЦОД та відновити своєчасну роботу ЦОД у випадку успішної реалізації кібератаки.

У даній роботі було проведено аналіз застосування методів кластеризації масивів даних ЦОД для забезпечення інформаційної безпеки комплексу. Кожен з методів характеризується, складністю, типом даних, які кластеризує, а також вхідними і вихідними параметрами реалізації алгоритму на його основі.

Серед п’яти вказаних методів кластеризаціїї найбільш ефективним вважається метод поєднання часткової класифікації та наївних баєсівський класифікатор. Гібридна техніка, яка поєднує аналіз непрогнозованого сигналу мережевих функцій і векторну машину підтримки, дозволяє порівняти ефективність методів та виявити аномалії у мережі на найбільш ранніх стадіях.

СПИСОК ЛІТЕРАТУРИ

1. Jain A., Murty M., Flynn P. Data Clustering: A Review. // ACM Computing Surveys. 1999. Vol. 31, no. 3.
2. Mauricio Arregoces, Maurizio Portolani // «Data Center Fundamentals» // Cisco Press. 2003.
3. Бериков В. С., Лбов Г. С. Современные тенденции в кластерном анализе // Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы» — 2008.
4. Згурский А. С. Метод и модель формирования системы обеспечения информационной безопасности центра обработки данных кредитных организаций — 2011.
5. Котов А., Красильников Н. Кластеризация данных — 2006.
6. Мандель И. Д. Кластерный анализ. — М.: Финансы и статистика, — 1988.

ОСОБЛИВОСТІ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ НА ПРИКЛАДІ ЦИФРОВІЗОВАНИХ ОБ’ЄКТІВ ЕЛЕКТРОЕНЕРГЕТИКИ

Гільгурт С.Я.,[1] Щербина В.П.[2]
[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
[2]Національний авіаційний університет

Цифровізація критичної інфраструктури разом з перевагами стандартизації та підвищення якості комунікації привносить проблеми кібернетичної небезпеки, притаманні традиційним інформаційним підходам. Але наслідки від реалізації атак на об’єкти критичної інфраструктури можуть бути більш важкими, навіть катастрофічними в порівнянні з традиційними галузями IT-технологій [1, 2]. Ситуація в галузі захисту інформації кіберфізичних систем поки залишається на початковому етапі. Отже, питання аналізу особливостей вирішення завдань інформаційної безпеки щодо автоматизованих і автоматичних систем управління на виробництві, зокрема, в енергетиці, є актуальними та

злободенними. В даній роботі досліджено особливості вирішення задач інформаційної безпеки електричних цифрових підстанцій (ЦПС). При цьому головну увагу приділено протоколам обміну даними, що використовуються, та їх захисту від зовнішніх атак.

Електричні підстанції є одними з найчисленніших об'єктів енергетики [3]. Складнощі, що виникають при переводі їх обладнання на цифрову елементну базу, пов'язані в першу чергу зі стандартизацією. Якщо життєвий цикл силового обладнання, такого як трансформатори, комутаційні апаратні роз'єднувачі тощо складає близько 40 років, то керуючі системи оновлюються в середньому кожні 15 років. В результаті змушені спільно взаємодіяти пристрої декількох поколінь, не сумісні між собою. Для вирішення даної проблеми було створено стандарт МЕК 61850 «Мережі та системи зв'язку на підстанціях» [4], який завдяки застосуванню єдиних специфікації дозволяє, з одного боку, захистити фінансові вкладення в енергетичне обладнання, з іншого – задіяти переваги передових обчислювальних та комунікаційних технології. Оснований на використанні цифрових вимірювальних приладів і так званих інтелектуальних електронних пристроїв – Intelligent Electronic Devices (IED), комплекс нормативів МЕК 61850 впевнено асоціюється у фахівців з такими поняттями як "цифрова підстанція" та Smart Grid.

Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів [5]:

– станційний (Station Level) – найвищій рівень;

– рівень приєднання (Bay Level);

– рівень процесу (Process Level) або "польовий" (Field Level) – найнижчий рівень.

Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

Станційний рівень забезпечує людино-машинний інтерфейс з персоналом, який керує підстанцією, і включає системи моніторингу, автоматизовані робочі місця (АРМ) та SCADA-системи.

Рівень приєднання в режимі реального часу виконує всі автоматичні функції з керування станцією, що не потребують втручання людини, включаючи функції контролю, вимірювання, синхронізації часу та захисту (аварійної автоматики). Реалізують всі ці функції інтелектуальні пристрої IED, які пов'язують станційний рівень з польовим, надаючи пристроям рівня станції можливість зчитувати та записувати інформацію з нижчого рівня.

Рівень процесу включає як звичайне (застаріле), так і сучасне електричне обладнання (рубильники, пускачі, вимірювальні трансформатори тощо). Сучасні кінцеві пристрої здатні безпосередньо передавати інформацію через Ethernet. Звичайне ж обладнання нові стандарти передачі даних не підтримує, тому для зв'язку з ним на рівні процесу використовують додаткові компоненти, такі як Merging Units (MU) та Intelligent Terminals (IT) [6].

На додаток до традиційних протоколів, таких як FTP або HTTP, стандарт МЕК 61850 вводить нові протоколи, а саме:

– MMS (Manufacturing Message Specification) – для зв'язку IED зі станційним рівнем;

– GOOSE (Generic Object Oriented Substation Events) – для зв'язку IED між собою;

– SV (Sampled Values) – для зв'язку між IED та MU.

Строго кажучи, MMS є не протоколом, а специфікацією, що описує інформаційну модель пристроїв та даних рівня приєднання. Але, оскільки сервіс, що використовує MMS, застосовує рівень додатків стандартного стеку мережевих протоколів OSI, його також можна умовно вважати протоколом обміну. Принаймні, в технічній літературі з питань використання стандарту МЕК 61850 та вирішення проблем захисту інформації у системах Smart Grid на його основі, скорочення MMS в переважної більшості публікацій згадується саме як протокол.

Достатньо змістовний опис згаданих протоколів, включаючи часові діаграми, можна знайти в літературі, наприклад, в [6]. Зауважимо, що в кіберфізичних системах, побудованих на базі стандарту МЕК 61850, також можуть використовуватися інші мережеві протоколи, наприклад, поширена польова шина MODBUS, або її проприєтарна модифікація MODBUS Plus, протокол часової синхронізації PTP (Precision Time Protocol), протокол

виявлення мережевих пристроїв LLDP (Link Layer Discovery Protocol) та ін. Але в даному дослідженні йдеться саме про MMS, GOOSE і SV.

Як свідчить аналіз багатоадресних протоколів, до яких належать GOOSE та SV, існує дев'ять основних шляхів використання їх вразливостей з метою порушення роботи компонентів енергосистеми [7]:

1) компрометація інтерфейсу користувача;
2) переривання процесу синхронізації часу;
3) компрометація шини зв'язку на станційному рівні;
4) отримання доступу до пристроїв рівня приєднання;
5) зміна налаштувань захисного пристрою;
6) захоплення та модифікація повідомлень протоколу GOOSE;
7) компрометація комунікаційної шини на рівні процесу;
8) розміщення підроблених значень у повідомленнях протоколу SV;
9) компрометація міжмережевого екрану для отримання доступу до мережі підстанції.

Незалежно від перелічених способів використання вразливостей, існують певні варіації здійснення конкретної атаки. Нижче перелічені типи різновидів атак з описами, а також потрібні заходи протидії [6].

1. Дублювання (Replay) – старі повідомлення передаються повторно – перевірка узгодженості атрибутів.
2. Безпосереднє вкидання (Naive injection) – передаються сфабриковані повідомлення (команди для GOOSE або виміри для SV) – стандартна перевірка цілісності за стандартом МЕК 61850.
3. Вкидання МЕК 61850 (IEC 61850 injection) – передаються сумісні з МЕК 61850 шкідливі команди (GOOSE) або повідомлення з фальшивими вимірами (SV) – перевірка узгодженості атрибутів контексту (GOOSE) або кореляція вимірювань кількох джерел (SV).
4. Маскування (Masquerade) – передаються повідомлення, що імітують реальну поведінку – перевірка узгодженості та кореляції.
5. Псування (Poisoning) – поле StNum надмірно збільшене – перевірка узгодженості атрибутів.
6. Модифікація (Modification) – фальшиві атрибути – перевірка узгодженості атрибутів.
7. Flood-атака (Flooding) – багато повідомлень передаються з високою частотою – перевірка статистики повідомлень.

Оскільки протокол MMS використовує на рівні додатків стандартний стек мережевих протоколів, на нього можуть здійснюватися всі типи атак, притаманні протоколам IT-галузі.

Як свідчать дослідження, методологія боротьби з кіберзагрозами, що традиційно використовується в IT-сфері, не в повній мірі може бути застосована для кіберфізичних систем на базі стандарту МЕК 61850 [8]. Цифрові пристрої, що використовуються в Smart Grid, мають обмежені обчислювальні ресурси. У таких пристроях важко оновлювати ПЗ та firmware, використовувати традиційні міжмережеві екрани та антивіруси [3]. Системи виявлення вторгнень, особливо їх програмні реалізації, які орієнтовані на традиційні комп'ютери, також недостатньо ефективні в промислових мережах.

З іншого боку, аналіз показує, що існує можливість в процесі розпізнавання шкідливої активності враховувати фізичну інфраструктуру кіберфізичних систем. Якщо традиційні IT-комунікації є різнорідними і в широких межах варіюються за своєю природою, систем промислової автоматики мають певну сталу структуру і типові шаблони комунікації, які слід брати до уваги при виявленні підозрілої активності [8]. Тобто, можливість врахування структурної специфіки можна розглядати як перевагу промислових систем, зокрема, ЦПС перед інформаційними об'єктами в плані захисту інформації. Якщо, наприклад, в трафіку між двома конкретними вузлами промислової мережі відповідно до структури інформаційних обмінів повинні бути присутніми пакети лише деяких конкретних протоколів, то система виявлення вторгнень має інтерпретувати будь-які інші пакети як зловмисні та видавати попередження про вторгнення [3].

Отже, засоби цифровізації, такі як стандарт МЕК-61850, надають багато переваг системам промислової автоматизації, впроваджують нові протоколи та функціональні можливості. Але нова якість таких систем, на жаль, призводить до збільшення загроз кібербезпеки, реалізація яких може привести до катастрофічних наслідків. Для їх захисту можна використовувати відомі системи виявлення вторгнень, але після певного адаптування. Досліджені особливості побудови цифрових підстанції на основі стандарту МЕК-61850 дозволяють виявити певні переваги в плані кіберзахисту в порівнянні з інформаційно-комунікаційними додатками.

СПИСОК ЛІТЕРАТУРИ

1. Assante M.J. Confirmation of a Coordinated Attack on the Ukrainian Power Grid / M.J. Assante // SANS Institute, Bethesda, USA (January 6, 2016) [Електронний ресурс]. – Режим доступу: https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid. – Загл. з екрану. – (Дата звернення: 15.05.2021)
2. Sanger D.E. Cyberattack Forces a Shutdown of a Top U.S. Pipeline / D.E. Sanger, C. Krauss, N. Perlroth // The New York Times (May 8, 2021) [Електронний ресурс]. – Режим доступу: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html. – Загл. з екрану. – (Дата звернення: 15.05.2021)
3. Multi-attribute SCADA-specific intrusion detection system for power networks / Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E.G. Im, B. Pranggono, H.F. Wang // IEEE Trans. on Power Delivery. – 2014. – Vol. 29, P. 1092-1102.
4. Communication Networks and Systems in Substations, IEC Std. 61850, 2003.
5. Аналіз зарубіжної практики впровадження автоматизованих систем управління технологічними процесами в електроенергетиці / Міністерство енергетики та вугільної промисловості України, ДП «НЕК «Укренерго», Науково-технічний центр електроенергетики. – К.: 2014. – 113 с.
6. A survey on intrusion detection and prevention systems in digital substations / S.E. Quincozes, C. Albuquerque, D. Passos, D. Mossé // Computer Networks. – 2021. – Vol. 184. – Article 107683.
7. Hong J. Detection of cyber intrusions using network-based multicast messages for substation automation / J. Hong, C. Liu, M. Govindarasu // IEEE conf. on Innovative Smart Grid Technologies (ISGT), IEEE: 2014. – P. 1-5.
8. Multidimensional intrusion detection system for IEC 61850-based SCADA networks / Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, S. Sezer // IEEE Trans. Power Deliv. – 2017. – Vol. 32, № 2. – P. 1068-1078.

КІБЕРБЕЗПЕКА ТА СТІЙКІСТЬ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Гнатюк С.Є.
Адміністрація Державної служби спеціального зв'язку та захисту інформації

Анотація. *Розглядаються питання кібербезпеки та стійкості електронних комунікацій користування в умовах подальшої цифровізації та інформатизації процесів в рамках «Цифрова держава» та «Цифрове суспільство». Визначається необхідність створення умов для збільшення рівня стійкості та сталості процесів в умовах зростання впливу кібернебезпеки, кіберзлочинів та кіберінцидентів. Вказане повинно відбуватися при тісній співпраці держави та приватного бізнесу у контексті сформованих заходів із забезпечення системою стійкості та сталості усього спектру інфраструктури, і розпочати треба із критичної інфраструктури електронних комунікацій.*

Розвиток інформаційно-комунікаційних технологій разом із подальшою цифровізацією інформації, інформаційних комунікативних процесів, а також широке впровадження програм та проектів з інформатизації формують нові умови до подальшої широкої цифровізації в рамках «Цифрова держава» та «Цифрове суспільство». Так в Україні останніми роками Урядом країни здійснюються практичні кроки щодо переведення комунікацій на рівні громадянин-держава (в частині надання адміністративних послуг, доступу до баз даних та цифрових ресурсів) в онлайн режим. Крім того більшість електронних послуг можна отримати на одній онлайн платформі, що покращує якість надання послуг та комунікацій. Крім того в багатьох сферах економіки, у промисловості та сферах обслуговування впроваджуються програми та проекти з інформатизації, автоматизації (впровадження штучного інтелекту, Інтернет-речей та запуск і експлуатація програм Smart Sity). Основною транспортною складовою усіх сучасних процесів цифровізації є електронні комунікації, а тому від їх безперебійного функціонування залежать усі подальші процеси, які формуються на базі телекомунікаційних послуг. Отже ми стаємо свідками, коли в більшості питання управління критичною інфраструктурою відбувається за допомогою ІКТ, автоматизованих мережевих систем управління, віддаленого доступу та формування багаторівневих інформаційно-телекомунікаційних систем. В таких умовах питання стійкості та сталості функціонування як вказаних систем, так і самих об'єктів критичної інфраструктури набуває актуальності та потреби у збільшенні рівня до такого стану, щоб функціонування відбувалося з високим ступенем залишкового резерву. Особливо питання стійкості та сталості систем набуває в рамках кібернебезпеки, кіберінцидентів.

Вирішення питань стійкості та сталості в умовах кібернебезпеки потребує комплексного, фахового, універсального та всеохоплюючого підходу, що може бути тільки в умовах формування та реалізації відповідної державної політики, де держава повинна виступити суб'єктом усіх процесів. Так, на сьогодні ведуться заходи з розроблення, затвердження та впровадження Концепції національної стійкості. Крім того окрім окреслення концептуального бачення та розуміння суті проблеми та шляхів їх вирішення, необхідно разом і концепцією розробляти План заходів із реалізації заходів щодо національної стійкості по окремим напрямам, сферах, об'єктам.

Так, Стратегія національної безпеки України (далі – Стратегія) «ґрунтується на таких основних засадах: стримування; стійкість; взаємодія та прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України», де стійкість розглядається як «здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема шляхом мінімізації зовнішніх і внутрішніх вразливостей»[5]. Група дослідників, розглядаючи питання економічної стійкості визначають стійкість як «здатність системи зберігати свій стан щодо досягнення запланованих результатів за наявності різних впливів збурення» навіть коли «збурення можуть викликати тимчасові відхилення координат стану системи у межах заздалегідь визначених допусків, але з припиненням впливів стійка система має повертатися у вихідне положення»[2]. Зважаючи на вказане можна говорити про те, що в «Україні нині притаманний високий рівень ризиків і загроз практично в усіх сферах – внутрішній і зовнішній, соціально-економічній і суспільно-політичній, воєнній, екологічній та інших. Має місце багато уразливостей через недостатній рівень консолідації суспільства, неефективність державного управління, незавершеність реформування сектору безпеки і оборони та процесів децентралізації, системні вади національної економіки тощо» [4, с.4], що потребує необхідності побудови національної системи стійкості. Адже як показує досвід усіх років існування низький рівень національної системи стійкості є нестабільним і не забезпечує стабільне існування системи (політичної, економічної, соціальної тощо). Це в свою чергу впливає на рівень національної безпеки і кібербезпеки. Крім того необхідно враховувати подальше включення нашої країни у глобалізаційні процеси та вплив глобальних світових гравців, транснаціональних компаній, глобальних ЗМІ тощо. Вказане суттєво впливає на рівень національної стійкості як в цілому, так і в окремих сферах. Формування сталої

національної системи стійкості є досить довгим процесом у часі та вимагає значних ресурсів і консенсусу на рівні громадянин-суспільство-держава. А беручи до уваги певну тотожність розуміння системи національної безпеки та національної стійкості, можна говорити про певне їх поєднання для економії ресурсів та комплексного підходу до процесів взаємодії на рівні державно-партнерських взаємовідносин між державними структурами та інституціями, приватним бізнесом, громадянським суспільством. Як показує практика та досвід країн, де вже здійснюється комплексний підхід до вирішення питань стійкості, до побудови національної стійкості застосовуються два підходи: широкий та вузький. Так, під «широким підходом» розуміється «коли принципи стійкості імплементуються в усі сфери національної безпеки і державного управління, включаючи економічну, соціальну, екологічну, суспільну, міжнародну та інші», а під «вузьким» - «за основу береться вдосконалення кризового менеджменту у сфері захисту населення і критично важливих об‘єктів держави від різних загроз і небезпек (передусім, природного, техногенного, біологічного, терористичного або воєнного характеру), а також безперервності виконання критично важливих функцій держави (зокрема, урядування, постачання енергії, води і продуктів харчування, транспортного сполучення і зв‘язку, надання первинної медичної допомоги, здатності впоратися з масовим переміщенням людей або значними людськими втратами тощо)»[4, с.3]. Зважаючи на реалії нашої країни, при побудові національної стійкості необхідно використовувати «широкий підхід», а також враховувати, що «для реагування на нові загрози (особливо гібридного типу) мають бути запропоновані нові механізми, побудовані за принципами національної стійкості»[3, с.174].

Так, М. Каліман в рамках Концепції забезпечення національної стійкості пропонує виділити загрози та ризики (за джерелом їх настання) національної, а саме: «загрози та ризики природного, техногенного та соціального характеру»[1, с.197]. Також М. Каліман в рамках Концепції пропонує виділити п’ять питань, які потребують вирішення, а саме: відсутність принципів законності та верховенства права серед переліку принципів функціонування національної системи стійкості; відсутність визначення видів загроз та ризиків національній безпеці; відсутність у складі державних органів уповноваженого суб’єкта оцінювання загроз національній безпеці; відсутність алгоритмів дій суб’єктів національної стійкості за умов загрози чи виникнення надзвичайних ситуацій; відсутність діяльності органів та підрозділів Національної поліції України як базового елементу національної системи стійкості»[1, с.196].

Підсумовуючи можна відзначити таке. Зважаючи на фінансово-економічний та соціально-політичний стан розвитку України питання формування національної системи стійкості необхідно виходити із того, що одразу охопити усі аспекти неможливо, а тому треба розпочати із критичної інфраструктури і поступово розширювати включати до національної системи стійкості наступні сфери, сектори та взаємовідносини за рівнями (від національного до місцевого), враховуючи перш за все загрози та ризики природного, техногенного та соціального характеру. Перш за все необхідно вирішити питання стійкості електронних комунікацій, як основної транспортної основи інформаційних процесів та процесів подальшої цифровізації та інформатизації.

Вказані заходи повинні бути сформовані в рамках Плану заходів із реалізації заходів щодо національної стійкості по окремим напрямам, сферах, об’єктам. Для підвищення ефективності вказані заходи необхідно здійснювати на державно-приватному рівні взаємовідносин, коли і держава і бізнес беруть участь у створенні та функціонуванні національної системи стійкості.

СПИСОК ЛІТЕРАТУРИ

1. Каліман М.Р. Деякі питання вдосконалення процесу забезпечення національної стійкості в Україні. Юридичний науковий електронний журнал. № 3/2021. С.196-198.

2. Козловський С.В., Рудковський О. В., Козловський А. В. Концепція управління стійкістю сучасної економічної системи як основа забезпечення її розвитку. Економіка та держава № 12/2017, С.4-8.

3. Резнікова О. Забезпечення національної безпеки і національної стійкості: спільні і відмінні риси. Вісник Львівського університету. Серія філос.-політолог. студії. 2018. Випуск 19, С.171-175.

4. Резнікова О.О., Войтовський К.Є. Щодо концепції забезпечення національної стійкості в Україні. НІСД. Аналітична записка Серія «Національна безпека», № 8, 2020, 11 с.

5. Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 року № 392/2020. URL : https://www.president.gov.ua/documents/3922020-35037. (Дата звернення 10.06.2021).

МЕТОДИКА ОЦІНКИ ВПЛИВУ ІНФОРМАЦІЙНИХ ЗАГРОЗ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Бутвін Б.Л. , Штифурак Ю.М., Сидоренко О.В.
НТУУ "КПІ ім. І. Сікорського"

Однією з важливих задач досягнення належного рівня забезпечення кібербезпеки є виявлення та оцінка рівня інформаційних загроз для сучасних інформаційних мереж держави, а також їх впливу на національну безпеку України. Тому розробка методики оцінки впливу інформаційних загроз на національну безпеку України є досить важливою науково-практичною задачею. Одним з напрямів рішення цієї задачі є застосування сучасних інформаційних технологій на основі інтелектуального аналізу даних, розробка спеціального програмного забезпечення на основі застосування сучасного математичного апарату, який дозволить адекватно оцінити інтегральні рівні загроз національній безпеці України з урахуванням етапу розвитку інформаційних загроз, їх масштабу і наслідків для різних сфер діяльності держави. Емпіричні підходи, які використовуються у наш час, не повною мірою дозволяють вирішити поставлену задачу. Одним із перспективних напрямів вирішення цієї задачі є застосування методології нелінійного багатофакторного оцінювання поточних інформаційних загроз національній безпеці України на основі метамоделі, що визначає актуальність і новизну наукової задачі, яка розглядається у тезах.

Одним з центральних понять цього методичного підходу є поняття метамоделі. У загальному вигляді під метамоделлю будемо розуміти модель, яка описує структуру, принципи побудови інших моделей.

У контексті задачі, яка розглядається у даній роботі, під метамоделлю розуміємо складну ієрархічну багатофакторну нелінійну аналітичну (а також алгоритмічну) модель опису та розрахунку інтегрального рівня (індексу) загроз національній безпеці України.

Але слід відзначити, що типові інформаційні загрози мають різні масштаби, етапи та наслідки для життєво важливих інтересів України.

У теперішній час вже існує аналітична методика оцінки інтегрального рівня загроз національній безпеці України. У даній методиці використовується мультиплікативна згортка часткових показників оцінки з урахуванням етапу, масштабу та наслідків інформаційних загроз для різних сфер національної безпеки України. Але це можливо тільки за умови незалежності цих показників один від одного. Це твердження не є достовірним, бо ці часткові показники загроз певним чином впливають один на одного, що обмежує практичне застосування цієї методики для взаємовпливових загроз.

Для усунення цього протиріччя пропонується методичний підхід розрахунку інтегрального рівня інформаційних загроз на основі нелінійної багатофакторної ієрархічної метамоделі.

Позначимо інтегральний рівень інформаційної загрози у наступному вигляді (формула 1):

$$K_з = F\{EP_з(t), X(t), F_i(НЗ_к(t))\}, \quad (1)$$

де:

$F(*)$ – функціонал розрахунку інтегрального рівня (індексу) інформаційної загрози;

$EP_з(t)$ – показник урахування етапу розвитку інформаційної загрози;

$X(t)$ – показник урахування масштабу розвитку інформаційної загрози;

$F_i(НЗ_к(t))$ – інтегральний показник наслідків впливу інформаційної загрози на і-ту сферу.

Інтегральний показник наслідків впливу інформаційної загрози на і-ту сферу матиме наступний вигляд (формула 2):

$$F_i(НЗ_к(t)) = F_1\{НЗ_1(t), НЗ_2(t), НЗ_3(t), НЗ_4(t), НЗ_5(t)), \quad (2)$$

де:

$НЗ_1(t)$ – інтегральний показник наслідків впливу інформаційної загрози на першу сферу;

i – від 1 до 5.

Для розрахунку функціоналів $F(*)$ було застосовано сучасний метод групового урахування аргументів, який забезпечує досить високу адекватність та достовірність розрахунку інтегрального показника впливу інформаційних загроз на показники національної безпеки України. На рис. 1 наведено статистичні оцінки якості побудови аналітичного функціоналу (метамоделі), а на рис. 2 – внесок складових загроз на інтегральний показник.

Результаты подготовки данных	Обучение	Экзамен
Число наблюдений	8	2
Макс. отрицательное отклонение	-0.152827	-0.166332
Макс. положительное отклонение	0.109348	0.271024
Средний модуль ошибки (MAE)	0.0813266	0.218678
Среднеквадратическое отклонение (RMSE)	0.0958252	0.224856
Сумма отклонений	3.33067E-16	0.104692
Стандартное отклонение остатков	0.0958252	0.218678
Коэффициент детерминации (R^2)	0.850748	0.640461
Корреляция	0.92236	1

Рис.1. Статистичні оцінки якості побудови аналітичного функціоналу (метамоделі)

Внесок | Частота

№	Якщо замістити середнім значенням	Вплив на СКВ	Графічно	СКВ
1	H_тер, cubert	63,36%		0,812581
2	H_сувер, cubert	55,98%		0,764484
3	Етап, cubert	41,90%		0,672805
4	Характер, cubert	40,96%		0,666664
5	H_добр, cubert	31,23%		0,603329
6	H_духов, cubert	22,62%		0,547228
7	H_умови, cubert	16,54%		0,507685
	[Нічого не заміщено]	0%		0,399946
	[Заміщено все]	100%		1,05117

Рис.2. Внесок складових загроз на інтегральний показник

Таким чином, метод побудови метамоделі оцінки інтегрального рівня інформаційних загроз на основі методу групового урахування аргументів слід розглядати як практичний підхід

до вирішення задачі розробки методики оцінки впливу інформаційних загроз на національну безпеку України.

АНАЛІЗ ТОПОЛОГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНСЬКОГО НАЦІОНАЛЬНОГО ГРІДУ

Корченко О.Г., Давиденко А.М., Висоцька О.О.
Національний авіаційний університет

Нестримний розвиток засобів високопродуктивних обчислень породив багато варіантів обчислювальних архітектур і технологій, прикладом яких є суперкомп'ютери такі як Tianhe-2, Titan – Cray XK7, Sequoia – Blue Gene/Q, K Computer, Mira – Blue Gene/Q та багато інших. Більшість цих комп'ютерів об'єднує масово-паралельна архітектура яка побудована із множині процесорів зв'язаних в єдину обчислювальну мережу. Для звичайних користувачів більш доступні хмарні та грід мережі, експлуатація яких не потребує бюджету супердержави. Якщо суперкомп'ютер це місто в якому замість хмарочосів стоять стойки з електронікою, то грід система це одна вулиця, яка об'єднує приблизно 1000 процесорів поєднаних в три - чотири стойки або взагалі будинок з 24 обчислювальних нод.

Основною перевагою грід систем є можливість об'єднання ресурсів для вирішення ресурсномістких обчислювальних завдань, що мають виконуватися нерегулярно [1-6]. При цьому існує протиріччя між бажанням отримати максимальну продуктивність і необхідністю забезпечення інформаційної безпеки. Проаналізуємо сучасний стан даної проблеми з метою визначення актуальних шляхів її вирішення [7]. Грід-системи першого покоління створювалися переважно на принципах довіри один одному та адміністративними одиницями - дослідними лабораторіями та академічними інститутами. Globus Alliance (міжнародний консорціум дослідників грід) разом з іншими науковими і комерційними організаціями працював на основі Open Grid Services Architecture (OGSA). Ця архітектура [8-10] визначає механізми для створення, найменування і пошуку файлів на основі грід-служб.

Архітектура захисту інформації в грід-службах забезпечує виконання широкого колу завдань безпеки – від випадків в яких вимоги до захисту мінімальні або зовсім не має, до задач з високого рівня вимогами до забезпечення конфіденційності, цілісності та доступності.

Грід-служби об'єднують різні адміністративні домени, в кожному з яких є особистий автономний механізм захисту. Архітектура безпеки забезпечує протоколи, що дозволяють компенсувати відмінності між автономними механізмами, і при цьому надає кожному локальному вузлу повний контроль над ресурсами, які відносяться до нього.

Загальним для засобів безпеки грід систем є принципи захисту [1,8]:

— Автентифікація - надання способу підключення різних механізмів автентифікації і методу їх використання в різних ситуаціях;

— Передача прав - надання засобів, що дозволяють здійснювати передачу прав доступу від запитуючої сторони до служби, що викликається;

— Одноразовий вхід - звільнення суб'єктів, які виконали процедуру автентифікації, від необхідності її повторення при кожній спробі доступу до ресурсів на деякий час;

— Життєвий цикл мандатів і його оновлення - у багатьох випадках можлива ситуація, коли процес, ініційований суб'єктом, виконується довше, ніж час дії виданого мандата. Тому необхідно попередження про це суб'єкта або передбачити оновлення мандата, для того щоб робота могла бути закінчена;

— Авторизація - дозвіл доступу до служб на підставі політик авторизації, пов'язаних з ними (хто і на яких підставах може здійснювати доступ), і надання можливості стороні, що викликає, задавати політики виконання (кому клієнт довіряє виконання);

— Конфіденційність - запобігання витоку (розголошенню) будь-якої інформації;
— Цілісність даних - забезпечення виявлення несанкціонованих змін;
— Обмін політиками - надання можливості обміну інформацією про політику безпеки сторін, що викликає і викликана, для створення безпечного середовища обміну інформацією.
— Рівень забезпечення безпеки - реалізація засобів, що дозволяють визначити необхідний рівень забезпечення безпеки системи;
— Проникність мережевих екранів (firewalls) - основним бар'єром при передачі даних в динамічних, кросдоменних Grid - систем є міжмережеві екрани, тому при проектуванні системи необхідно забезпечити можливість вільної передачі даних через екран без зміни їх політик безпеки.

Більшість з перерахованих вище принципів увійшли в стандарт під назвою OGSA (Security Architecture for Open Grid Services), розроблений Open Grid Forum (OGF), і на сьогоднішній день Globus Toolkit (GT) є широко поширеною реалізацією цього стандарту.

Апаратною базою реалізації дослідження було обрано елементі Українського національного гріду (УНГ), тому розглянемо топологію організації інформаційної безпеки внутрішнього.

Основними елементами УНГ є [1-4]:
— ресурсні центри національного рівня;
— Центр сертифікації з регіональними філіями;
— Центр реєстрації віртуальних організації;
— Центр моніторингу грід-інфраструктури та реєстрації грід-сайтів;
— грід-сайти - вузли УНГ, що підключені до національної грід-інфраструктури.

Координацію роботи для підтримки, функціонування УНГ проводить Базовий координаційний грід-центр Українського національного гріду і регіональні координаційні грід-центри.

Автентифікація в грід-системі реалізована з використанням програмного продукту NorduGrid [5,10] і використовує сертифікат відкритого ключа X.509 [2] інфраструктури відкритих ключів [3]. В процесе реалізації санкціонованого доступу проміжне програмне забезпечення NorduGrid від імені автентифікованого користувача запускає на ідентифікованому кластері розподілений програмний застосунок користувача (РППЗ). Зазвичай РППЗ використовує інтерфейс передавання повідомлень Message Passing Interface (MPI) [4] для організації обміну повідомленнями в розподіленому середовищі, а конкретний екземпляр РППЗ виконується в операційної системі (ОС) конкретного обчислювального вузла. Схемі взаємодії РППЗ, NorduGrid і MPI мають високу динаміку змін, тому для них необхідне динамічне формування вимог безпеки. З іншого боку, операційні та мережеві середовища мають традиційні функції і складають основу безпеки, для них існують типові вимоги, оскільки від них залежить безпека функціонування грід-середовища в цілому зазвичай з них формується політика безпеки. Але це породжує протиріччя між звичайними однопотоковими механізмами захисту інформації та паралельним середовищем основою якого є архітектура MPI.

Актуальною версією проміжного програмного забезпечення (ППЗ) ARC [6,7,9] в УНГ на початок 2021 року є версія 5.0.2. В процесі аналізу розглянуто його реалізацію, а саме підсистемі які є його складовими. Це є наступні грід-служби: Керування завантаженням; Керування даними; Інформаційне забезпечення; Безпека і контроль прав доступу; Протоколювання; Обчислювальний елемент.

Вимоги щодо забезпечення інформаційної безпеки в гріду можна згрупувати в чотири множини. Це вимоги до автентифікації, управління обліковими записами користувачів, реагування на інциденти безпеки та моніторингу. Забезпечення цих вимог потребує певних механізмів захисту.

Механізми автентифікації для грід-сайту повинні забезпечувати:
— єдиний вхід – користувач повинен зареєструватися і автентифікуватися тільки один раз на початку сеансу роботи, отримуючи доступ до всіх санкціонованих ресурсів ґрід - сайту;

— делегування прав – користувач повинен мати можливість запуску власних програм від свого імені. Має бути забезпечено доступ програми до всіх ресурсів санкціонованих для користувачу. Особисті програми можуть, при необхідності, делегувати частину своїх прав іншим програмам.

Механізми управління обліковими записами користувачів для грід-сайту повинні забезпечувати:

— контроль унікальності ідентифікатору та паролю (атрибуту) в рамках операційної системи грід-сайту на підставі відповідного сертифіката користувача;

— контроль за безпекою паролів, яка включає перевірки якості процедур генерування та збереження;

— блокування облікових записів;

— реєстрацію дій по створенню, модифікації та віддаленню облікових записів.

Механізми реагування на інциденти безпеки для грід-сайту повинні забезпечувати можливість контролювати небезпечні дії шляхом розпізнавання, фіксації та аналізу дій і подій, пов'язаних з дотриманням політики безпеки інформації.

Механізми моніторингу для грід-сайту повинні забезпечувати:

— функціонування журналів реєстрації дій адміністраторів і користувачів, а також неполадок, що виникають в процесі обробки інформації.

— перевірку вжитих заходів і верифікацію їх відповідності політиці доступу.

— збереження протягом погодженого періоду журналу аудиту, для сприяння в майбутніх розслідуваннях і моніторингу контролю доступу.

— контроль за переглядом на регулярній основі журналів реєстрації адміністраторами грід-сайту.

— захист інформації та засобів її реєстрації від фальсифікації та несанкціонованого доступу.

Проведення аналізу цих служб а особливо механізмів автентифікації та управління обліковими записами користувачів дозволило показати протиріччя між звичайними однопотоковими механізмами захисту інформації та паралельним середовищем основою якого є архітектура MPI, що застосується для реалізації процедур розпаралелювання в грід-системах. Також оцінено продуктивність кластерів УНГ. Отримані дані показують істотне зростання пікової продуктивності до 3712 Гфлоп. При мінімальній продуктивності 16 Гфлоп. Для EGI показники будуть ще більше. Збільшення продуктивності веде до збільшення розриву з однопотоковими механізмами захисту.

СПИСОК ЛІТЕРАТУРИ

1. Украинский академический грид / А.Г. Загородний, Г.Е. Зиновьев, Е.С. Мартынов, С.Я. Свистунов – Українсько-македонський науковий збірник.: Випуск 4, Київ – 2009, Вид. Національна бібліотека України імені В.І.Вернадського, С.140-150.

2. ПОЛОЖЕННЯ про Український Національний Грід (УНГ) [Електронний ресурс]. – Режим доступу: http://infrastructure.kiev.ua/upload/ung_fin.pdf.

3. ПРАВИЛА використання ресурсів Українського Національного Гріда (УНГ) [Електронний ресурс]. – Режим доступу: http://infrastructure.kiev.ua/upload/ resources_fin.pdf.

4. ПОЛОЖЕННЯ про Базовий координаційний грід-центр Українського Національного Гріду [Електронний ресурс]. – Режим доступа: http://infrastructure.kiev.ua/ upload/bcc_fin.pdf.

5. Advanced Resource Connector // NORDUGRID [Електронний ресурс]. – Режим доступу: http://www.nordugrid.org/arc.

6. Інсталяція ARC2 [Електронний ресурс]. – Режим доступа: http://grid.org.ua/wiki/ tech/arc1.

7. UA-Grid: Украинская национальная грид-программа / А.Г. Загородний, С.Я. Свистунов, Л.Ф. Белоус, А.Л. Головинский // International Conference "Parallel and Distributed Computing Systems" PDCS 2013(Ukraine, Kharkiv, March 13-14, 2013), pp.346-356

8. Практикум з грід-технологій: навчальний посібник / А.І. Петренко, С.Я. Свістунов, Г.Д. Кисельов – К.: НТУУ «КПІ», 2011. – 580 с.
9. UGRID. Ukrainian Academical grid monitoring [Електронний ресурс]. – Режим доступу: https://194.44.37.211/nagios.
10. Advanced Resource Connector // NORDUGRID [Електронний ресурс]. – Режим доступу: http://www.nordugrid.org/arc.

ОГЛЯД ІСНУЮЧИХ МЕТОДИК ВИЯВЛЕННЯ DDOS-АТАК

Кравчук А.А.
НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»

З високошвидкісними DDoS-атаками можна впоратись, використовуючи, на приклад, метрику ентропії конкретних полів пакетів. Даний спосіб є найбільш популярним і використовуваним поміж інших для даного роду атак. У статті [2] детально описується алгоритм виявлення вторгнень: скануються усі вхідні пакети, збирається з них така інформація, як: IP-адреса джерела, час надходження, обчислюються певні характеристики розподілу та однорідності адрес і порівнюються із зразковим набором даних легітимного трафіку. Загалом це можна описати формулою $\left|E(s_i) - E(s_j)\right| \geq \delta$, де E – це певна функція, яка характеризує інформаційну ентропію IP-адрес, s_i та s_j – це набір даних про вхідний трафік за певну визначену одиницю часу під час ймовірної атаки та під час її відсутності відповідно, а δ – певний поріг однорідності адрес, під час перевищення якого будуть блокуватися найбільш повторювані IP-адреси. Загалом описаний метод успішно виявляє такі атаки, як-от: UDP-флуд, HTTP-флуд, SYN-флуд тощо. Перевагою є висока точність виявлення зловмисного трафіку (близько 94%), відносно мала обчислювальна складність, завдяки чому можна досить швидко в режимі реального часу аналізувати трафік без залучення великих обчислювальних ресурсів, низька ймовірність позитивно помилкового визначення. Проте даний спосіб має достатньо недоліків: неможливість виявлення низькошвидкісних атак, відсутність чіткого та очевидного критерію для встановлення порогового значення, який відповідальний за класифікацію шкідливого трафіку. Використання показника інформаційної ентропії IP-адрес є не достатнім для виявлення усіх видів DDoS-атак, доцільніше його використовувати разом із ще одним ефективним методом, який би визначав також низькошвидкісні типи атак.

Одним із таких методів, який би міг виявляти низькошвидкісні DDoS-атаки, є метод *k*-найближчих сусідів (або ж KNN, від англ. *k*-nearest neighbor), який описаний у статті [3]. Він базований на використанні методів машинного навчання, а основний принцип полягає в тому, що клас досліджуваного об’єкта визначається найбільш поширеним класом серед найближчих *k* об’єктів. Для цього необхідно обчислювати відстань за певною формулою, враховуючи як можна більше факторів про поточний трафік. Загалом з отримуваних пакетів можна отримати такі данні, як: кількість надісланих байтів, тип протоколу, адреса відправника, адреса та порт призначення тощо. Також окрім цього, застосовуючи, наприклад, метод рухомого вікна і виокремлюючи дані про трафік за певний проміжок часу, можна розрахувати деякі додаткові характеристики: кількість пакетів з даного джерела до сервера, кількість активних з’єднань певного протоколу та інші. Таким чином з обраних n характеристик можна сформувати Евклідовий простір R^n, де конкретний пакет x в певний момент часу можна представити вектором його характеристик $\left(f_1(x) \quad f_2(x) \quad \ldots \quad f_n(x)\right)$, а відстань можна обчислити за Евклідовою нормою. На основі отриманих класів можна виділяти окремі підозрілі групи зі схожою поведінкою, які суттєво впливають на трафік, і відповідно до цього приймати рішення щодо їх блокування. Загалом даний метод у порівнянні із попереднім досить добре виявляє низькошвидкісні DDoS-атаки, але при цьому має певні недоліки, а саме: відносно значний

відсоток (близько трьох) хибного виявлення шкідливого трафіку. Це зумовлене тим, що досить поширеною є ситуація, коли відстань до більшості *k* найближчих сусідів є майже однаковою, і це створює проблеми із правильною класифікацією поточного пакету.

Також одним із популярних методів машинного навчання, яким би можна було виявляти DDoS-атаки, є метод опорних векторів (або ж SVM, скор. від англ. support vector machine). У статті [4] зазначається, що даний метод може класифікувати об'єкти досить точно при невеликих обсягах даних для тренування. Основною ідеєю є пошук так званої розділової гіперплощини із найбільшим проміжком між двома класами, що представлені об'єктами – *n*-вимірними векторами. Для використання даного методу необхідно попередньо натренувати модель на зразкових даних. Цей набір даних повинен виглядати наступним чином: $D = \{(\overline{x}_1, y_1), (\overline{x}_2, y_2), ..., (\overline{x}_n, y_n)\}$, де $\overline{x}_i$ є вектором з даними, які характеризують певний пакет, а y_i – вказує на приналежність даного пакету до певного класу (наприклад, зі значенням 1 – шкідливий трафік, а з 0 – нормальний). На відміну від попереднього методу, SVM має значно менший відсоток хибно позитивних маркувань DDoS-атак, а також здатен виявляти такі підвиди низькошвидкісних атак, як-от: slowread, slowloris.

У статті [5] описується використання багатошарового перцептрону Румельхарта (або ж MLP, від англ. multilayer perceptron), який належить до класу штучних нейронних мереж прямого поширення, для виявлення DDoS-атак. У такому типі нейронних мереж дані розповсюджуються в одному напрямку, починаючи з вхідного шару нейронів, далі сигнал проходить через приховані шари до вихідного шару, де і формується остаточний результат. Загалом процес знаходження атак на відмову в обслуговуванні можна розбити на три модулі: модуль навчання, який відповідає за тренування моделі на основі зразкових даних з відповідною класифікацією, модуль виявлення та модуль коригування. Модуль виявлення відповідальний за класифікацію поточного вхідного трафіку, використовуючи логістичну функцію активації виду $f(x) = \left(1 + e^{-x}\right)^{-1}$ для даної штучної нейронної мережі. Далі вихідний шар класифікує результат як нормальний або шкідливий трафік на основі отриманої ймовірності. Для методу зворотного поширення помилки використовується функція перехресної ентропії. Модуль коригування в режимі реального часу може доповнювати набір зразкових даних завдяки новим отриманим класифікаціям і такими чином тренувати наявну модель на цих даних. У роботі [6] порівнюється декілька методів виявлення DDoS-атак (серед них є і ті, що були описані вище) в одних і тих самих умовах і на основі цього стверджується, що MLP має найвищу точність знаходження серед інших, що і є головною перевагою даного методу. Єдиним вагомим недоліком є те, що для використання багатошарового перцептрону необхідно виділити достатньо велику кількість обчислювальних ресурсів.

Висновки: в даній статті було розглянуто та проаналізовано декілька популярних методів виявлення DDoS-атак. Встановлено, що штучні нейроні мережі, а саме багатошаровий перцептрон Румельхарта, мають досить високу точність виявлення низькошвидкісних атак. Для покриття більшості видів атак на відмову в обслуговуванні бажано застосувати в парі з попереднім методом ще один спосіб виявлення на основі метрики інформаційної ентропії. Щоби заощадити кошти на придбанні додаткових обчислювальних ресурсів, можна контейнеризувати запропоноване рішення і розподілити навантаження серед робочих серверів за допомогою системи оркестровки контейнерних рішень, наприклад Kubernetes.

СПИСОК ЛІТЕРАТУРИ

1. Fakieh, K. An Overview of DDOS Attacks Detection and Prevention in the Cloud [Text] / International Journal of Applied Information Systems. — 2016. — Vol. 11, № 7. — P. 25 – 34.

2. Bhuyan, M.H. E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric [Text] / M.H. Bhuyan, D. K. Bhattacharyya, J.K. Kalita // Security and Communication Networks. — 2016. — Vol. 9, № 16. — P. 3251 – 3270.

3. Dong S. DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks [Text] / S. Dong, M. Sarem // IEEE Access. — 2020. — Vol. 8. — P. 5039 – 5048.

4. Ye J. A DDoS Attack Detection Method Based on SVM in Software Defined Network [Text] / J. Ye, X. Cheng, J. Zhu // Security and Communication Networks. — 2018. — Vol. 2018, Article ID 9804061.

5. Wang M. A dynamic MLP-based DDoS attack detection method using feature selection and feedback [Text] / M. Wang, Y. Lu, J. Qin // Computers & Security. — 2020. — Vol. 88. — p. 101645. — ISNN 0167 4048.

6. Pérez-Díaz, J.A. A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning [Text] / J.A. Pérez-Díaz, I.A. Valdovinos, D. Zhu // IEEE Access. — 2020. — Vol. 8. — P. 155859 – 155872.

СИСТЕМАТИЗАЦІЯ МЕТОДІВ СТЕГОАНАЛІЗУ ДЛЯ АУДІОСИГНАЛІВ

Г.В. Мартинюк, В.В. Козловський, К.С. Нестеренко, Т.В. Мелешко, І.І. Яковів
Національний авіаційний університет

Анотація. *Наводяться методи стегоаналізу, які застосовуються для різних форматів аудіосигналів. Розглядається типова система для виявлення факту приховання повідомлення. На основі аналізу сучасної літератури та проведення експериментів обгрунтовано найбільш розповсюджені методи стегоаналізу, наведено їх переваги та недоліки.*

Стеганографія стає все більш популярною в зв'язку із швидким зростанням цифрового контента і широко поширеною системою зв'язку в Інтернеті. Цифрове зображення високої чіткості і аудіосигнал, максимально наближений до звуків природи, можна отримати зручним способом за допомогою цифрової камери і цифрового диктофона [1]. На сьогодні існує велика кількість сервісів, які навіть доступні в Інтернеті, за допомогою яких можна вбудувати повідомлення в зображення, аудіо- чи відеофайл. Отже, існує можливість зберігання своїх секретних даних у цифровому контенті, після чого їх можна відправляти або зберігати на своїх дисках для забезпечення конфіденційності.

Перевагою стеганографічних методів є те, що тільки цільові одержувачі стегоконтейнера можуть отримати приховане повідомлення. Третя сторона не буде знати про наявність прихованих даних у повідомленні. Але необхідно відмітити, що стеганографічні методи не завжди використовують «во благо» - за допомогою стеганографічних методів можна передавати інформацію про об’єкти критичної інфраструктури, а також різного роду секретну та таємну інформацію. На сьогодні відома ціла низка різних стеганографічних методів для приховування контейнерів у медіа файлах [2]. Для виявлення факту наявності прихованого повідомлення користуються методами стегоаналізу. Типова система стегоаналізу має вигляд, зображений на рис. 1.

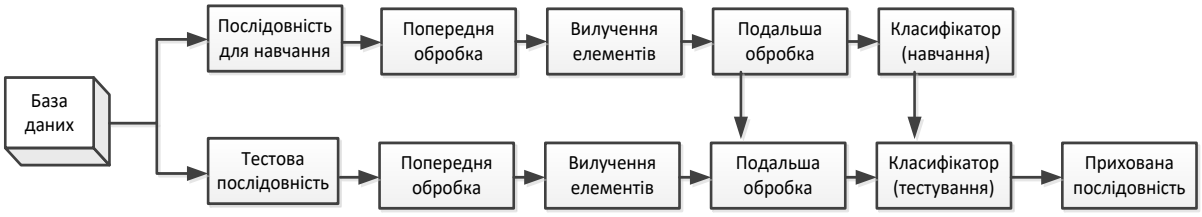


Рис.1. Блок-схема типової системи стегоаналізу

Аналіз аудіофайлів на наявність внесених змін - це процес, що дозволяє оцінити внутрішню структуру файлу на предмет обробки будь-якої програмою [3]. Необхідно сказати, що ця область розвивається активно, на сьогодні вже розроблено ціла низка різних методів стегоаналізу, які можна використовувати на практиці (рис.2).

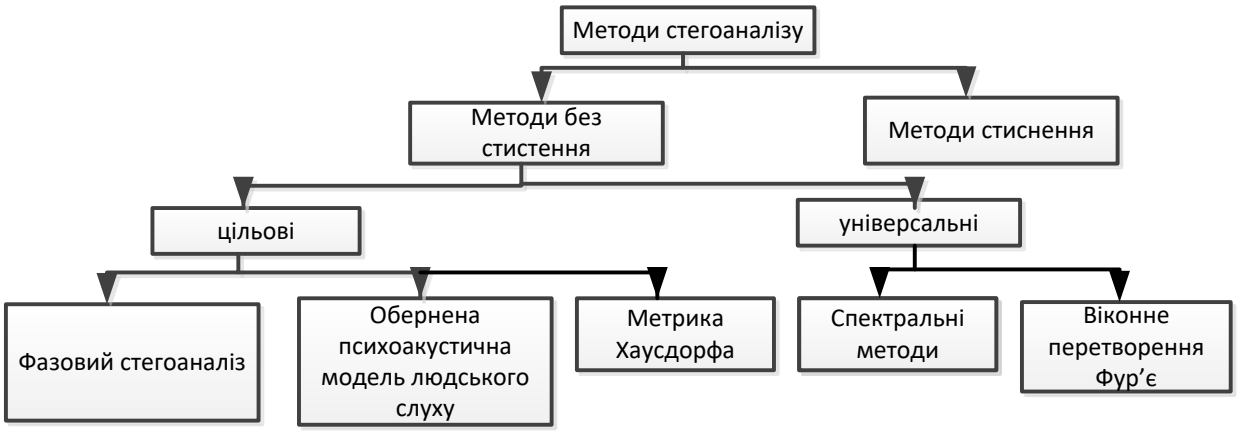


Рис.2. Загальна класифікація методів стегоаналізу аудіосигналів

Більш детально розглянемо наведені на рис. 2 методи [4].

Методи стиснення. При використанні алгоритмів стиснення вихідний порожній контейнер стискається, як правило, краще, ніж заповнений. Значить, якщо ступінь стиснення передбачуваного контейнера більше деякого порогового значення, то з великою ймовірністю можна сказати, що контейнер порожній, в іншому випадку можна говорити про присутність повідомлення в контейнері. Такі методи полягають в порівнянні коефіцієнтів стиснення вихідного контейнера і його повністю заповненої копії. До обох файлів застосовується метод стиснення даних, і аналізуються їх коефіцієнти стиснення. Якщо ці коефіцієнти близькі за значеннями, то з великою ймовірністю можна стверджувати, що вихідний файл містив приховане повідомлення, інакше йдеться про відсутність секретної інформації в об'єкті.

Метод фазового стегоаналізу. Даний метод використовується як метод стегоаналізу, якщо приховане повідомлення вбудоване у контейнер методом модифікації фази аудіосигналу. За допомогою методу фазового стегоаналізу знаходять зміну абсолютного значення фази деяких гармонік. Існують різновиди метода, в яких відновлюються значення різниць фаз суміжних фреймів. Робиться це на основі припущення, що людина сприймає ні абсолютних значення фази сигналу, а різницю фаз суміжних фрагментів. В інших методах фаза обраної гармоніки змінюється або на фіксоване значення, або змінюється знак дійсної і уявної частин комплексного спектра. Для детектування секретної інформації в аудіосигналі необхідно проаналізувати розподіл значень квадрантів фаз гармонік. У разі якщо у фрейм було вбудовано повідомлення, буде помітна перевага деяких квадрантів.

Обернена психоакустична модель людського слуху. Даний метод використовується як метод стегоаналізу, якщо приховане повідомленя вбудовано у контейнер за допомогою методу зміни часу затримки ехо-сигналу. Кількісна оцінка звуку по висоті заснована на статистичній обробці великого числа даних про суб'єктивне сприйняття висоти звукових тонів. Необхідно відмітити, що даний метод має ряд значних недоліків. По-перше, даний метод погано справляється при наявності адитивного шуму. По-друге, при використанні даного методу є можливість втрати даних аудіосигналу.

Метрика Хаусдорфа. Даний метод умовно можна назвати універсальним, так як його можна використовувати для різних методів стеганографії. Проте використання конкретного правила виявлення прихованої інформації безпосередньо залежить від алгоритму вбудовування, що є недоліком в плані універсальності. Якщо алгоритм невідомий для користувача, то виявлення прихованого повідомлення може бути ускладнене. Метод заснований на знаходженні максимально-мінімального відношення між вихідним контейнером та його заповненою копією.

Віконне перетворення Фур'є. Даний метод являє собою метод стегоаналізу, заснований на аналізі природних закономірностей записаного мовлення. За допомогою частотно-часового розкладу сигналу, останній описується в базисних функціях, які локалізовані по часу та частоті. Віконне перетворення Фур'є є найбільш поширеним частотно-часовим розкладом для аудіосигналів. Даний метод дозволяє з високою ефективністю виявляти вкладення різними стандартними методами. При цьому розглянутий метод не завжди зможе виявляти зміни в записаній музиці. Також з'являються ускладнення використання методу для різних форматів аудіосигналів через широкий спектр їх відмінностей.

Спектральні методи. Спектральний аналіз полягає в переведенні аудіосигналу з часової форми в частотну для більш зручного розгляду вмісту та визначення змін між близько розташованими даними. Виявлення прихованого повідомлення відбувається за допомогою знаходження статистичних характеристик аудіосигналу, переведеного в частотну область. Недоліками методів спектрального аналізу є те, що ймовірність правильного виявлення прихованого повідомлення при використанні методів стеганографії складає 50 % [5].

Висновки. У роботі приділена увага методам стегоаналізу, які використовуються для аудіосигналів. Наведено загальну класифікацію методів стегоаналізу, проаналізовано їх переваги та недоліки.

СПИСОК ЛІТЕРАТУРИ

1. M. D. Hassan. Sound based Steganalysis for Waveform Audio File Format (WAV) and Audio File Format (AU) / M. D. Hassan, M. A. Mohammed Amin, S. Mahdi // Journal of Electronic Systems. - Volume 8 Number 3. – 2018. – p. 103-111.
2. R. Din. Review on Steganography Methods in Multi-Media Domain / R. Din, M. Mahmuddin, A. J. Qasim // International Journal of Engineering & Technology, 2019 – № 8 (1.7). – p. 288-292.
3. Конахович Г.Ф. Компьютерная стеганография. Теория и практика [Монография] / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: "МК-Пресс", 2006. – 288 с.
4. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
5. Гераськин А.С. Обнаружение скрытого стеганографического вложения и признаков монтажа в области данных аудиофайла / А. С. Гераськин, Е. Д. Смирнов // Вестник ВГУ, серия: системный анализ и информационные технологии. – 2020. - № 2. – С. 69-78.

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ ЗНЕВОДНЕННЯ БІШОФІТУ З МЕТОЮ АНАЛІЗУ КРИТИЧНИХ СКЛАДОВИХ

Іванченко Є.В., Політучий О.О., Скворцов С.О.
Національний авіаційний університет

Вступ. Дослідження є розвитком попередніх робіт[1, 2], що спрямовані на видобуток корисних копалин та їх переробку. В результаті виконаних робіт була пробурена свердловина № 1 Затуринського родовища бішофіту (хлористий магній MgCl2x6H2O) де був застосований вказаний програмно-апаратний комплекс. На протязі тривалого часу і до тепер продукцією видобутку являється водний розчин вказаного мінералу, який використовується в гірничо-видобувній та нафтогазовій промисловості в медицині та агрокомплексі. Вперше в Україні ТОВ «Мінерал» виконало геологорозвідувальні роботи, захистило запаси в державному комітеті запасів, отримало ліцензію на видобуток, обсяги яких на сьогодні становить 18 тисяч тон на рік. Одним з недоліків продукції є великий вміст води, який становить 70%, а це суттєво збільшує витрати на її транспортування. Відомі методи випарювання потребують великих енергетичних витрат.

Мета дослідження полягає у дослідженні проекту програмно-технічного комплексу для контролю, оптимізації та управління технологічним процесом видобутку сухого хлориду магнію шляхом випарювання його з водного розчину. Контроль та управління планується здійснювати джерелом водяного пару, чотирма теплообмінниками, двома реакторами, кристалізатором та системою охолодження та водозабезпечення.

Основна частина. Об'єктом дослідження е проект технічного комплексу, який дозволяє підігріти водний розчин бішофіту до температури 120 C^0, забезпечити його циркуляцію через плівочний випаровувач, в якому концентрація доводиться до 37%. Потім в реакторі концентрація доводиться до 47%, і на барабанному кристалізаторі отримується кінцевий продукт.

Весь технічний комплекс оснащується датчиками тиску, температури, рівня та продуктивності. В комплексі передбачається система управління установкою, яка призначена для автоматизованого управління технологічним процесом переробки хлор магнієвих розсолів в кристалічний бішофіт. При цьому система повинна забезпечувати:

– збір і первинну переробку інформації,

– контроль і сигналізацію відхилення від норм технологічних параметрів;

– позиційну сигналізацію стану двигунів технологічного обладнання;

– автоматичне регулювання параметрів установки;

– дистанційне керування регулюючої арматури та відображення інформації;

– блокування роботи механізмів установки при досягненні меж аварійних уставок технологічних параметрів;

– подачу звукового та світлового сигналу при виході технологічних параметрів станції за допустимі межі з індикацією цього параметра на панелі оператора і моніторі комп'ютера системи верхнього рівня.

Управління механізмами установки

Система повинна передбачати два режими управління механізмами установки – місцевий та дистанційний. Місцевий режим здійснюється з поста управління (крім насосів рециркуляції, відсічних клапанів, а також регулюючих клапанів) за допомогою кнопок «Пуск» і «Стоп». Перехід до місцевого режиму здійснюється безпосередньо на посту управління перекладом перемикача у відповідне положення.

У дистанційному режимі управління виконавчими механізмами здійснюється з панелі оператора програмно-технічного комплексу. Переключення механізму в дистанційний режим можливий тільки з поста управління перекладом перемикача в відповідне положення.

Стан виконавчих механізмів повинно відображатися надписами і значками на панелі оператора і моніторі програмно-технічного комплексу. Більшість виконавчих механізмів установки використовуються як регулюючі органи у відповідних контурах регулювання. Відповідно управління ними проводиться автоматично в залежності від стану виходу регулятором, але початковий пуск таких механізмів повинен виконуватися оператором в ручному режимі, і тільки після такого запуску дані механізми повинні починати працювати в контурах автоматичного регулювання.

Проведемо аналіз та декомпозицію [3] схеми технологічного процесу з метою аналізу критичних складових.

Основна мета декомпозиції – поділ системи на частини, які мають меншу складність, з метою забезпечення умов для аналізу підсистем для вдосконалення систем управління [4].

Відомі напрямки декомпозиції автоматизованих систем управління дозволяють виділити структурні, функціональні, етапні, поелементні та інші підсистеми АСУ ТП [5-7].

Існують різні напрямки розбиття систем, але кожний з напрямків декомпозиції АСУ має своє певне призначення:

– структурний напрямок дозволяє отримати порівняно незалежну підсистему або комплекс завдань для кожного підрозділу або групи всередині підрозділів;

– функціональний напрям дає можливість створювати підсистеми або групи завдань виконуваних функцій управління процесом;

– поділ на функції другого роду дозволяє отримати спеціалізовані підсистеми для управління складними оригінальними операціями;

– людино-машинний підхід дає можливість виділити в проекті людські фактори і апаратну частину. Наприклад, техніку безпеки, умови ефективного функціонування людини та ін.;

– напрямок автоматизації виділяє підсистеми, які зручно описувати в проекті. У них містяться загальні правила, які стосуються до багатьох підсистем. Це дозволяє не повторювати ці матеріали в інших розділах проекту, а також уніфікує підходи у всіх підсистемах;

– напрям забезпечення, як і функціональній, дозволяє виділити підсистеми за профілем роботи фахівців, транспортників, енергетиків, постачальників та ін., проте в число забезпечуваних ресурсів слід віднести і всі види інформації, необхідної для управління, для чого будуть потрібні особливі фахівці та апаратура;

– напрямок етапів життєдіяльності системи дає можливість упорядкувати процеси розвитку і вдосконалення автоматизованої системи управління за допомогою відповідних підсистем, а при необхідності і процеси створення виробництв.

Аналізуючи підсистеми управління технологічних процесів першого рівня для обробки корисних копалин з урахуванням викладеного вище можливо довести, що запропонованій напрям не є повним.

Тому пропонується розширити перелік підходів предметно-орієнтованим підходом який базується на визначенні параметрів для декомпозицій на основі фізичної природи технологічного процесу. Наприклад, для техпроцесів, в яких здійснюється нагрів або охолодження, розділяти підсистеми, які використовують повітря, воду та пар за типом реагенту, що застосовується. На основі розглянутого підходу пропонується структурна схема системи керування технологічним процесом зневоднення бішофіту.

В результаті аналізу технологічного процесу з'ясувалося, що функції, які виконують центрифуга, кристалізатор і сушарка, можна реалізувати шляхом використання тільки кристалізатору барабанного типу. При цьому ускладнюється алгоритм керування (який в запропонованому програмно-технічному комплексі виконує програмований логічний контролер), проте скорочується склад використаного обладнання, знижується енергоспоживання та підвищується якість кінцевого продукту, оскільки кристалічний бішофіт отримується більш сухим і не потребує додаткової просушки.

Використання програмованого логічного контролера також дозволяє за рахунок більш точного керування технологічним процесом знизити вірогідність викиду хлору, що дає можливість знизити ризик шкідливого впливу виробництва бішофіту на довкілля.

Висновки. В роботі проведено аналіз технологічного процесу видобутку сухого хлориду магнію шляхом випарювання його з водного розчину. За рахунок удосконалення схеми автоматизованого контролю з’явилась можливість використання кристалізатору барабанного типу, завдяки чому буде зменшено енергоспоживання технологічного процесу та знижено ризики аварійного викиду хлору.

СПИСОК ЛІТЕРАТУРИ

1. *Давиденко А.М., Гільгурт С.Я., Політучий О.О.* Проблеми декомпозиції систем управління технологічним процесом на прикладі систем першого рівня // Зб. тез наук. доп. XI Всеукр. наук.-практич. конф. «Стан та удосконалення безпеки інформаційно-

телекомунікаційних систем (SITS'2019)». – с. Коблеве, 19-21 червня 2019 р.: збірник тез. – Миколаїв: 2019. – С.14-16.

2. *Давиденко А.М., Суліма О.А., Політучий О.О.* Реалізація процесів адаптації при вирішенні завдань захисту систем доступу до інформаційних об'єктів енергетики // Кібербезпека енергетики. – м. Одеса, 28 травня – 01 червня 2019 р.: збірка праць конференції. – Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2019. – С.16-20.

3. Патент UA 140326 U; G05B15/00, G05B19/00; Апаратно-програмний комплекс моніторингу та керування технологічним процесом зневоднення бішофіту / А.М. Давиденко, С.Я. Гільгурт, О.О. Політучій; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України. – заяв. u 2019 11509, 28.11.2019 р. – Опубл. 10.02.2020, Бюл. № 3.

4. *Бубліков А.В., Козарь М.В., Проценко С.М.*Автоматизація технологічних процесів підземних гірничих робіт: підручник / за заг. ред. В.В. Ткачова. - Дніпропетровськ.: НГУ, 2012.

5. *Шувалов В.В, Огаджанов Г.А., Голубятников В.А.* Автоматизация производтвеных процессов в химической промышленности. - М.: Химия, 1991

6. *Пантелеев А.В., Бортаковский А.С.* Теория управления в примерах и задачах: учебное пособие для вузов / А.В. Пантелеев,.– М.: Высшая школа, 2003. – 583 с.

7. О декомпозиции автоматизированных систем управления. Синтез подсистем автоматики // РИТМ [Електронний ресурс]. – Режим доступу: https://ritm.pro/dekompozicija-avtomatizirovannyh-sistem-upravlenija-sintez-podsistem-avtomatiki. – Загл. з екрану. – (Дата звернення: 14.05.2019).

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ БЕЗДРОТОВОГО ЗВ'ЯЗКУ АВІОНІКИ ПОВІТРЯНОГО СУДНА З ТОЧКИ ЗОРУ КОНЦЕПЦІЇ СІА

Поліщук С.Т.
Національний авіаційний університет

Цифрові обчислювальні машин та інформаційні технологій, що виникли у другій половини XX ст., набули широкого використання в усіх галузях народного господарства XXI ст. Науково-технічні досягнення у цьому напрямі суттєво впливали на економіки країн і призводили до кардинальних змін в житті людей. На сьогодні, проблема інформатизації всіх галузей господарства, в тому числі і авіаційної, є одним із пріоритетних напрямків для більшості країн світу, включаючи США, Великобританію, Німеччину, Японію та ін.

Проектанти авіаційної техніки завжди шукають способи зменшення ваги літака, підвищення потужності двигунів, зменшення витрачання палива, покращення аеродинамічних характеристик планера.Сучасні мікро- та нанотехнології досягли межи із зменшення ваги та енергоспоживання радіоелектронного обладнання повітряного судна (ПС).

Існуюча дротова технологія, яка використовує кабелі для з'єднання різних систем літака, крім збільшення ваги, також додає складність, пов'язану з надійністю, електромагнітною сумісністю, монтажем та обслуговуванням бортових систем (Рис. 1).

Наприклад, для літака A380-800 електрична проводка має наступні характеристики [**1**]:

- загальна кількість дротів ~ 100 000 шт.
- загальна вага проводів: ~ 5 700 кг
- близько 30% додаткової ваги для закріплення джгута на конструкції.

Тобто, близько 30% електричних проводів та 30% кріплення є потенційними кандидатами їх заміни на бездротовий радіо зв'язок!

На теперішній час, бездротові технології для бортових систем авіоніки мають ще дослідницький характер, (Рис. 2).

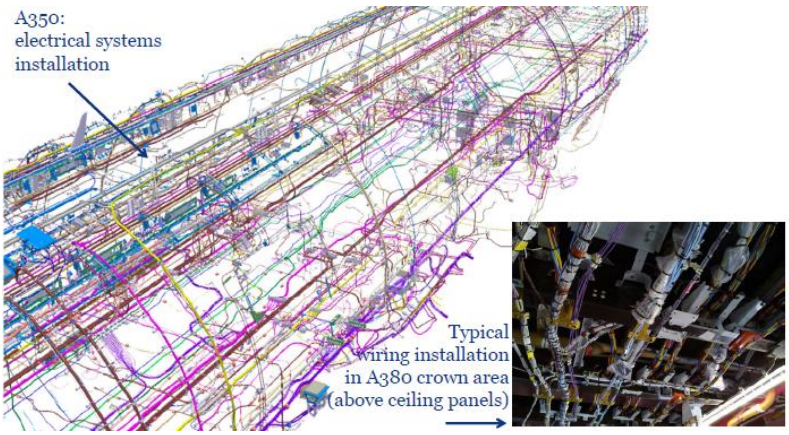


Рис. 1. Схематичне зображення електропроводки сучасного літака

Цей напрям має назву Wireless Avionics Intra-Communications (WAIC) - бездротова авіоніка внутрішньої комунікації [**2, 3, 4**].

Технологія WAIC може бути визначена як система бездротової комунікації, де мережеві пристрої або вузли розташовані на борту одного літака. WAIC спрямована на вирішення наступних завдань:

- створення датчиків з радіо інтерфейсами (wireless sensing);
- зменшення кількості кабельних з'єднань (cable replacement);
- структурний моніторинг стану динамічної системи (structural health monitoring);
- дистанційне керування та технічне обслуговування (remote control and maintenance).

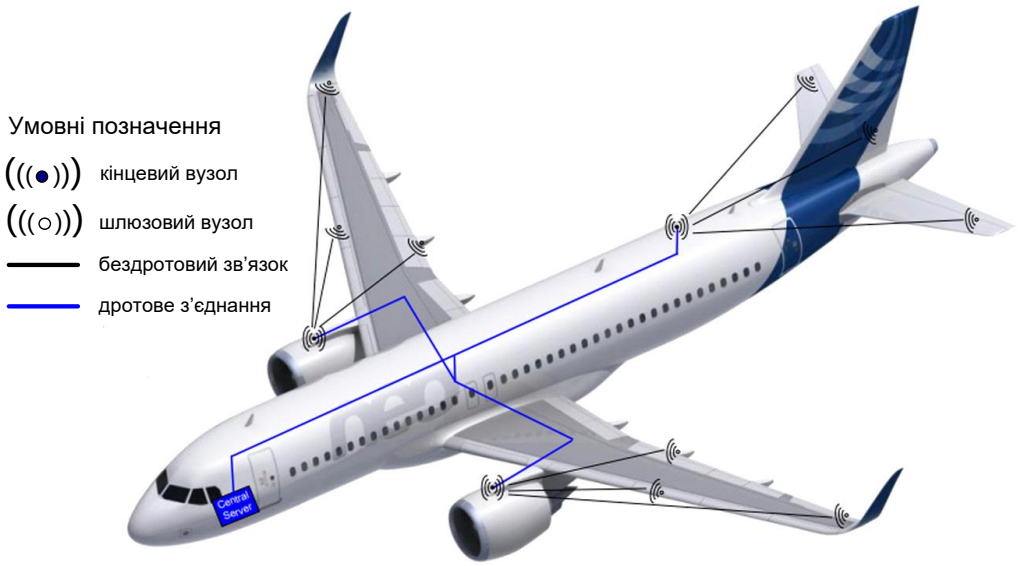


Рис. 2. Бездротовий зв'язок елементів системи керування ПС

Оскільки WAIC передбачає використання радіочастот, які також можуть використовуватися іншими пристроями, класифікація WAIC почалася з із співпрацею з Міжнародного союзу електрозв'язку (International Telecommunications Union, ITU). Крім того, оскільки радіосигнали систем WAIC випромінюються ПС, які переміщуються , перетинаючи міжнародні кордони, то для успішної класифікації в даному питанні потрібно співробітництво ITU з ІКАО.

ITU початково визначив робочий частотний спектр WAIC-пристроїв в межах від 2-х до 5-ти ГГц. У 2015 році ITU та ICAO вирішило виділити для технології WAIC діапазон частот 4.2 – 4.4 ГГц [**5**]. Неліцензований розподіл частот 2,4 ГГц і 5 ГГц спонукали індустрію зв'язку

розробити нові стандарти бездротового зв'язку. Серед них Bluetooth, ZigBee та Wi-Fi - це три найпопулярніші стандарти.

На *Рис. 3* наведено огляд різних бездротових стандартів, які знайдуть комерційне застосування. Стандарти розташовані в порядку збільшення швидкості передачі даних та потужності на осі X та збільшення робочого діапазону на осі Y.

Результати дослідження бездротових протоколів стандарту IEEE 802.11 в рамках європейського проекту «WILDCRAFT» (Wireless Smart Distributed End System for Aircraft) програми «Чисте небо» на частоті 2,4 ГГц наведено в таблиці.

У загальному розумінні безпека ПС означає захист наших систем та екіпаж та пасажирів від зловмисників, що можуть вторгнутися у мережі, стихійних лих, несприятливих умов навколишнього середовища, перебоїв з подачею енергії, крадіжок чи вандалізму чи інших небажаних станів.

Інформаційна безпека також визначається як "захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення **цілісності, конфіденційності та доступності**" [6]

Конфіденційність, що означає збереження дозволених обмежень доступу та розголошення, включаючи засоби захисту особистого конфіденційності та приватної інформації.

Цілісність, що означає захист від неналежного модифікування або знищення інформації, і включає забезпечення неповернення та достовірності інформації.

Доступність, що означає забезпечення своєчасного та надійного доступу до інформації та її використання

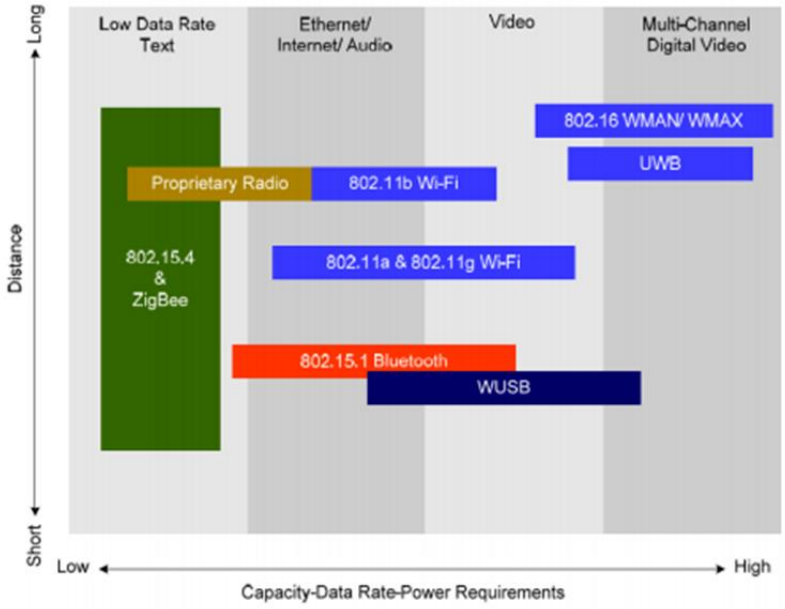


Рис 3. Порівняння бездротових стандартів за швидкістю передачі даних, енергоспоживанню і видалення вузлів [7]

Протоколи стандартів IEEE 802.11 (a, b, g)

Стандарт	**Тип модуляції**	**Частотний діапазон, ГГц**	**Швидкість передавання, Мвіт/с**	**Недоліки**
802.11a	OFDM	6, 9, 12, 18, 24, 36, 48, 54	Низький взаємний вплив в полосі частот. Високошвидкісний протокол	Велика вартість. Мала заповніність діапазону.

802.11b	DSSS DHSS	1,2, 5.5, 11	Велика дальність, низька вартість	Низькошвидкісний протокол
802.11g	OFDM DSSS	6, 9, 12, 18, 24, 36, 48, 54	Сумісність їх стандартом 802.11b	Більш заповнений діапазон

На теперішній час, з точки зору концепції безпеки CIA, майже відсутня інформація, яка б дозволяла фахівцям спрямовувати зусилля на втілення існуючих технологій підвищення інформаційної безпеки в авіаційної галузі.

СПИСОК ЛІТЕРАТУРИ

1. https://waic.avsi.aero/about/ Aviation Industry's Motivation
2. ITU.R M.2067 Technical characteristics and protection criteria for Wireless Avionics Intra-Communication systems.
3. ITU.R M.2319-0 (2014) Compatibility analysis between wireless avionicsintra-communication systems and systems in the existing services in the frequency band 4 200-4 400 MHz.
4. EUROCAE ED-246 Process Specification for Wireless On-board Avionics Networks.
5. Final acts WRC-15 world radio communication conference. GENEVA, 2015.
6. NIST SP 800-59 under Information Security from 44 U.S.C., Sec. 3542. https://csrc.nist.gov/glossary/term/INFOSEC
7. Satish Kumar Chilakala.- Development and Flight Testing of a Wireless Avionics Network Based on the IEEE 802.11 Protocols: Aerospace Engineering and the Graduate Faculty of the University of Kansas, 2008.- 165 p.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Потенко О.С., Корченко А.О.
Національний авіаційний університет

Надзвичайна складність сучасних інформаційних систем визначає різноманіття сучасних інформаційних моделей безпеки. Ці моделі описують певні аспекти інформаційної взаємодії. На сьогодні не існує єдиної моделі, яка описує всі існуючі нюанси інформаційної безпеки. Моделлю політики безпеки прийнято називати формальне описання політики безпеки для заданої системи. Інформаційні системи суттєво відрізняються одна від одної, тому і моделі повинні застосовуватись відповідні. Основними моделями безпеки інформаційної системи є [1-4]:

Модели систем дискретного розмежування доступу
- Take-Grant
- Модель Харрисона, Руззо та Ульмана

Модели систем мандатного розмежування доступу
- Модель Белла – ЛаПадула

Моделі контролю цілісності
-Модель Кларка –Вилсона

Інформаційні моделі
- Модель невтручання
- Модель невиводимості

Коротко розглянемо ці моделі виділяючи метод представлення даних та мету моделювання.

Модели систем дискретного розмежування доступу

Модель Take-Grant

Модель Take-Grant використовується для аналізу систем дискреційного розмежування доступу, у першу чергу для аналізу шляхів поширення прав доступу в таких системах. Як

основні елементи моделі використаються граф доступів і правила його перетворення. Ціль моделі - дати відповідь на питання про можливості одержання прав доступу суб'єктом системи на об'єкт у стані, описаному графом доступів. Зараз модель Take-Grant одержала продовження як розширена модель Take-Grant , у якій розглядаються шляхи виникнення інформаційних потоків у системах з дискреційним розмежуванням доступу. В моделі існує 4 правила:

– правило «Брати»
– правило «Давати»
– правило «Створити»
– правило «Видалити»

Методом представлення даних для даної моделі є граф доступу.

Метою моделювання являється аналіз шляхів поширення прав доступу.

Модель Харрисона, Руззо та Ульмана

В моделі Харрисона, Руззо та Ульмана захищена система складається з наступних елементів:

1. Кінцева множина загальних прав R = {r1, …, rn}:

2. Кінцевий набір початкових суб'єктів So та кінцевій набір об'єктів Oo, кожний суб'єкт являється також об'єктом.

3. Кінцеву множину команд C, представлених у формі:

command C(X1,X2,..., Xn), де C – имя, X1,X2,..., Xn – формальні параметрі, які вказують на об'єкт.

Матриця доступу може змінюватися за допомогою наступних операцій:

- enter r into (s, o)- введення права r у відповідний елемент M[s,o] матриці доступу;
- delete r from (s, o)- видалення права r з елементу M[s,o] матриці доступу;
- create subject s - створення суб'єкта s;
- destroy subject s - видалення суб'єкта s;
- create object o – створення об'єкта o;
- destroy object o – видалення об'єкта o.

Метод представлення даних є матрицею доступу.

Метою моделювання є представлення прав доступу.

Модели систем мандатного розмежування доступу

Модель Белла – Лапа дула

Модель Белла - ЛаПадула (Bell-LaPadula), призначена для керування суб'єктами, тобто активними процесами, що запитують доступ до інформації, і об'єктами, тобто файлами, поданнями, записами, полями або іншими сутностями даної інформаційної моделі.

В моделі об'єкти піддаються класифікації, а кожен суб'єкт зараховується до одного з рівнів допуску до класів об'єктів. Класи й рівні допуску спільно називаються класами або рівнями доступу.

Клас доступу складається із двох компонентів. Перший з них - це ієрархічний компонент. Другий компонент являє собою деяку множину неієрархічних категорій, які можуть ставитися до будь-якого рівня ієрархії.

Методом представлення даних є визначення двох компонентів. Перший з них - це ієрархічний компонент. Другий компонент являє собою деяку множину неієрархічних категорій.

Мета моделювання є керування суб'єктами, тобто активними процесами, що запитують доступ до інформації

Моделі контролю цілісності

Модель Кларка -Вилсона

В основі даної моделі лежить два принципи:

- Внутрішня цілісність
- Зовнішня цілісність

Модель реалізована за допомогою набора правил і не являється математичною моделлю. Також суб'єкти не мають прямого доступу до об'єктів, між ними знаходиться програма, яка має доступ до об'єктів. Контроль доступу розподілений таким чином, що тільки певні програми мають доступ до певних об'єктів, а суб'єкт має доступ тільки до певного набору програм.

Всі дані діляться на 2 класи:

- Необхідний елемент даних (CDI)
- Спонтанний елемент даних (UDI)

Далі створюється набір правил, які регулюють взаємодію з обома типами даних:

- Всі початкові процедури перевірки (IVP) повинні впевнитись в тому, що всі CDI знаходяться в достовірному стані під час роботи IVP.
- Всі процедури перетворення (TP), повинны бути сертифіковані.
- Правила доступу повинні задовольняти всім вимогам розподілення обов'язків.
- Всі процедури перетворення повинні бути записані в доступний тільки на дописування журнал.
- Будь-яка процедура перетворення, яка одержала вхід UDI повинна перетворити його в CDI інакше відмінити операцію.

Також для зміцнення захисту в системі існує ще додатковий набір правил. Цей набір забезпечує додатковий захист для процедур перетворення.

Метод представлення даних - необхідний елемент даних, спонтанний елемент даних.

Мета моделювання – створення набору правил, згідно з якими програма буде надавати або не надавати права певним суб'єктам.

Інформаційні моделі

Дані моделі є результатом застосування теорії інформації до проблеми безпеки систем. До інформаційних моделей ставляться моделі невтручання й невиводимості .

Достоїнствами даного типу моделей , на відміну від моделей надання прав , є:

- відсутність у них прихованих каналів витоку інформації ;
- природність їхнього використання для реалізації мережних захищених обчислювальних систем.

Модель невтручання

Модель невтручання розглядає систему, що складається з чотирьох об'єктів: високе введення (high-in), низьке введення (low-in), високе виведення(high-out), низьке виведення (low-out).

Розглянемо систему, виведення якої користувачеві *u* визначене функцією out(u, hist.read(u)), де hist.read(u) - історія введення системи (traces), чиє останнє введення було read(u) (команда читання , виконана користувачем u). Для визначення безпеки системи необхідно визначити термін очищення *(purge*) історій уведення , де *purge* знищує команди , виконані користувачем, чий рівень безпеки не домінує над рівнем безпеки u. Функція clearence(u) - визначає ступінь довіри до користувача.

Система задовольняє вимозі невтручання , якщо для всіх користувачів u, всіх історій T і всіх команд виведення з out(u,T.c(u)) = out(u,purge(u,T).c(u)).

Для того, щоб перевірити, чи задовольняє система вимогам невтручання, була розроблена множина умов («unwinding conditions»), виконання яких досить для підтримки невтручання в моделі.

Метод представлення даних - списки команд

Мета моделювання – визначення рівня довіри

Модель невиводимості

Розглянемо модель невиводимості, що також базується на розгляді інформаційних потоків у системі.

Система вважається невиведено безпечною, якщо користувачі з низькими рівнями безпеки не можуть одержати інформацію з високим рівнем безпеки в результаті будь-яких дій

користувачів з високим рівнем безпеки. Інакше кажучи, у таких системах витік інформації не може відбутися в результаті посилки високорівневими користувачами високорівневої інформації до низькорівневих користувачів. Інтуїтивно це визначення відноситься не до інформаційних потоків, а до поділу інформації. Однак таке визначення безпеки не захищає інформацію високорівневих користувачів від перегляду низькорівневими користувачами. Дане визначення вимагає, щоб низькорівневі користувачі не були здатні використати доступну їм інформацію для одержання високорівневої інформації (це пояснює, чому визначення назване невиводимістю).

Метод представлення даних є мітки доступу

Мета моделювання – запобігання перевищенню прав доступу

Таким чином розглянути моделі забезпечують широкий спектр представлення даних. Але розвиток обчислювальної техніки породжує нові інформаційні структурі, наприклад паралельні, тому актуальним є адаптація існуючих та розробка нових акцентованих на спеціалізованих сучасних структурах представлення даних.

СПИСОК ЛІТЕРАТУРИ

1. *Девянин П.Н.* Модели безопасности компьютерных систем – М.: Издательский центр «Академия», 2005. – 144 с.

2. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. – М.: Горячая линия - телеком, 2000. – 452 с

3. *Корт С.С.* Теоретические основы защиты информации. – М. : Гелиос АРВ, 2004. -240 с.

4. *Давиденко А.Н.* Математическое моделирование систем и средств защиты критической информации // Збірник наукових праць Інституту проблем моделювання в енергетиці НАН України, Львів «Світ», 1998 Вип4 – с. 109-113.

ПОПИТ НА ДОСЛІДЖЕННЯ ПО РОЗГОРТАННЮ DNSSEC В ІНТЕРНЕТІ

Приходько Т.Ю.[1], Козловський В.В.[2]
[1]ТОВ «Інтернет Інвест»
[2]Національний авіаційний університет

Система доменних імен (DNS) щодня використовується всіма, від приватних користувачів до державних органів влади, які підключаються до Інтернету, і майже всіма пристроями в Інтернеті. Технологія була створена задовго до того, як хто-небудь взагалі почав думати про мережеву безпеку. DNS працює без автентифікації і шифрування, тобто наосліп обробляє запити будь-якого користувача. З моменту її створення в 1983 році технологія все ще залишається вкрай вразливою до атак. Зокрема, на здатність зловмисників фальсифікувати відповіді на запити до DNS, тим самим дозволяючи перенаправляти кінцевих користувачів на веб-сайти під своїм контролем.

У відповідь на загрози, пов'язані з вразливістю DNS, міжнародна організація зі стандартизації IETF (https://www.ietf.org/) розробила DNSSEC - засіб для перевірки цілісності DNS-запитів. Іншими словами, DNSSEC може дати впевненість в тому, що відповідь на ваш DNS-запит не підроблена. Впровадження DNSSEC є не тільки кращою галузевої практикою, але також ефективно допомагає уникнути більшості атак на DNS. При використанні DNSSEC не запити і відповіді DNS підписуються ключем, а самі дані DNS підписуються власником цих даних. Застосування DNSSEC дозволяє забезпечити дві важливі функції в DNS:

- Перевірка справжності джерела даних дозволяє DNS-резолверу перевірити, чи дійсно отримані дані надійшли з тієї зони, звідки, як він вважає, вони мають бути.
- Перевірка цілісності даних дозволяє DNS- резолверу перевірити, чи не були ці дані змінені під час передачі, після того як власник зони підписав їх закритим ключем цієї зони.

Для правильної роботи протоколу DNSSEC повинні бути задіяні обидві його сторони: публікація, яка виконується власниками доменів, і пошук, який зазвичай виконується мережевими операторами, такими як інтернет-провайдери. Щоб від DNSSEC була користь, їх повинні використовувати обидві сторони [1].

Власники доменів, відповідальні за публікацію даних DNS, повинні забезпечити підписання своїх даних DNS за допомогою DNSSEC, для цього необхідно включити DNSSEC-підпис на своїх DNS-серверах (або у своїх реєстраторів) і передати реєстратору інформацію, що називається DS-записом.

Мережевим операторам потрібно всього лише включити перевірку DNSSEC на Резолверах, які обробляють DNS-запити для користувачів. Програмне забезпечення Резолверів все частіше включає перевірку DNSSEC за замовчуванням.

Тож здається, що для повноцінного розгортання DNSSEC потрібно виконати досить чіткі і на перший погляд прості завдання, оператори мережі мають здійснити включення перевірки DNSSEC, а власники доменів мають додати цифровий підпис до використовуваних ними імен.

То чому ж загальносвітовий рівень впровадження DNSSEC, який був розроблений понад 20 років тому, ледь досяг 20%, згідно статистичного аналізу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр).

Відповісти на це питання можливо, попередньо дослідивши масштаби розгортання DNSSEC у Інтернеті, починаючи з моменту запуску до сьогодення, проаналізувавши причини гальмування, що пов’язані з тими чи іншими технічними, економічними та адміністративними аспектами, як на рівні держав так і світовому рівні.

Щодо держав, як приклад державного регулювання питань розповсюдження DNSSEC в Україні, слід згадати Постанову Кабміну від 12 червня 2019 р. № 493 «Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади», в загальних положеннях якої наведено наступне: «Офіційний веб-сайт (веб-портал) органу виконавчої влади та офіційні веб-ресурси, що пов’язані з діяльністю органу виконавчої влади (далі - офіційний веб-сайт), повинні бути розміщеними в домені GOV.UA та у разі потреби у домені .УКР. Домен, на якому розміщений офіційний веб-сайт, повинен бути підписаний із застосуванням технології захисту доменних імен DNSSEC».[3].

Якщо в цифрах, то рівень перевірки DNSSEC загальносвітовий наведено на рис.1, та огляд у процентному співвідношенні країн Східної Європи наведено на рис.2, де Україна має третю позицію по розповсюдженню DNSSEC.

Code	Region	DNSSEC Validates
XA	World	25.43%
XE	Europe	34.52%
XC	Americas	30.20%
XF	Oceania	30.09%
XD	Asia	22.19%
XB	Africa	21.67%
XG	Unclassified	1.13%

Рис.1 Рівень перевірки DNSSEC по світу та регіонах. Вибірку отримано з офіційного ресурсу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр)

З наведеного, кількість користувачів DNSSEC зростає, але цього недостатньо, щоб уникнути атак, таких як серія міжнародних кампаній по захопленню DNS в 2018 і 2019 роках, що привела до появі першої в світі Директиви з надзвичайних ситуацій Агентства США з кібербезпеки і безпеки інфраструктури (US-CERT) і підштовхнула ICANN до повторного призову до всіх зацікавлених сторін повністю розгорнути DNSSEC [1]. Вже в травні 2021 року

Інтернет-корпорація ICANN опублікувала запит пропозицій (RFP), щоб знайти підрядника, здатного досліджувати масштаби розгортання DNSSEC у Інтернеті. [2]

CC	Country	DNSSEC Validates
CZ	Czech Republic, Eastern Europe, Europe	71.03%
PL	Poland, Eastern Europe, Europe	53.00%
UA	Ukraine, Eastern Europe, Europe	36.38%
RU	Russian Federation, Eastern Europe, Europe	30.10%
BG	Bulgaria, Eastern Europe, Europe	27.89%
SK	Slovakia, Eastern Europe, Europe	18.77%
MD	Republic of Moldova, Eastern Europe, Europe	10.57%
HU	Hungary, Eastern Europe, Europe	10.46%
BY	Belarus, Eastern Europe, Europe	10.39%
RO	Romania, Eastern Europe, Europe	5.41%

Рис.2 Рівень перевірки DNSSEC країн Східної Європи. Вибірку отримано з офіційного ресурсу регіонального інтернет-реєстратора APNIC (Азіатсько-Тихоокеанський мережевий інформаційний центр)

Робота охоплює такі завдання:

1. Вивчення академічної та галузевої літератури, пов’язаної з розгортання розширень безпеки DNS (DNSSEC).

2. Пошук і документування різних технік та показників, що використовуються для вимірювання DNSSEC розгортання, включаючи підписання, перевірку та будь-які інші відповідні заходи. Як метрику пропонується вказувати абсолютне значення, коефіцієнт або інший відповідний параметр.

3. Проаналізувати задокументовані метрики та рекомендувати, які метрики повинна мати організація ICANN, щоб отримати найбільш повне уявлення про стан розгортання DNSSEC.

4. Підготувати вичерпний звіт, в якому деталізувати висновки, включаючи детальну бібліографію усіх джерел, до яких звертались.

Повний текст запиту до світової спільноти, зацікавленої в забезпеченні стабільної, безпечної та відмовостійкої екосистеми DNS було опубліковано в документі Project Overview for the DNSSEC Deployment Metrics Research RFP [2].

Висновки: на сьогодні є актуальною необхідність в дослідженні масштабів розгортання DNSSEC у Інтернеті [4]. Безпека DNS повинна бути невід'ємною частиною плану по забезпеченню безпеки на всіх рівнях де використовується Інтернет, оскільки система, основним завданням якої є перетворення імен мережевих вузлів в IP-адреси, використовуються буквально всіма додатками і службами в мережі.

СПИСОК ЛІТЕРАТУРИ

1. DNSSEC: Защита DNS. [Електронний ресурс]. – Режим доступу: https://www.icann.org/en/system/files/files/octo-006-24jul20-ru.pdf

2. Project Overview for the DNSSEC Deployment Metrics Research RFP 17 May 2021. [Електронний ресурс]. – Режим доступу: https://www.icann.org/en/system/files/files/rfp-dnssec-deployment-metrics-research-17may21-en.pdf

3. ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ "Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади". [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/493-2019-%D0%BF#Text.

4. Запрос предложений: исследование показателей развертывания DNSSEC. [Електронний ресурс]. – Режим доступу: https://www.icann.org/ru/announcements/details/request-for-proposal-researching-dnssec-deployment-metrics-17-5-2021-ru.

5. Т.Ю. Приходько, И.О. Басюк. «Важность внедрения технологии DNSSEC безопасности Интернет-пользователей». Информационные и телекоммуникационные технологии: образование, наука, практика: тези доп. II Международной научно-практической конференции, 3 – 4 декабря 2015 г.,КазНТУ, г. Алматы — С.274-276.

КІБЕРБЕЗПЕКА ТА КІБЕРГІГІЄНА КОРИСТУВАЧІВ ПОСЛУГ НА БАЗІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Скибун О.Ж.
Адміністрація Державної служби спеціального зв'язку та захисту інформації

Анотація. *Розглядається питання кібербезпеки та кібергігієни користувачів послуг на базі електронних комунікацій. При цьому вартість доступу до електронних комунікацій та кінцевого обладнання постійно знижується, збільшуючи тим самим кількість потенційних споживачів комунікаційних послуг. Широке впровадження цифрових технологій та технологій, обладнання і програмного забезпечення передавання інформації у цифрових форматах за допомогою електронних комунікацій створює умови для зростання кількості послуг на базі електронних комунікацій. Крім того міжнародні електронні комунікації та глобальна мережа передачі даних стають основою для кіберпростору (віртуального простору), який все тісніше витісняє фізичний простір. Так, соціальні мережі та соціальні медіа переживають бурхливий розвиток і «втягують» до себе все більшу кількість людей. А це призводить до зростання кіберзагроз, кіберінцидентів та кібернебезпек, що потребує «підвищення рівня обізнаності громадян щодо небезпек в Інтернеті», «створення соціальних ініціатив, спрямованих на підвищення рівня цифрових навичок та цифрових компетентностей для представників різних цільових груп населення» [7] тощо.*

Стрімкий розвиток науки та техніки в сфері електронних комунікацій (технологій, мереж, програмного забезпечення, кінцевого програмованого обладнання споживачів) відкриває ще більше можливостей для цифровізації та інформатизації усіх сфер та процесів на глобальному, національному, регіональному та об’єктовому рівнях через збільшення переліку та обсягів надання послуг на базі електронних комунікацій. Так, міжнародні електронні комунікації та глобальна мережа передачі даних дають змогу передавати та отримувати інформацію (цифрову різних форматів) у реальному часі з усіх куточків світу, що створює глобальний віртуальний простір без національних кордонів та застережень на культурному, національному рівнях та на рівні віри і життєвого світу. Водночас подальше впровадження у широке користування програм та проектів «Цифрова держава» та «Цифрове суспільство», в рамках яких збільшуються обсяги інформації (цифрової), які передаються, отримуються, обробляються та зберігаються в інформаційно-телекомунікаційних системах державного та приватного рівнів (на різних платформах, базах даних та сервісах). Показовим є збільшення обсягів надання електронних адміністративних послуг через єдині платформи, комунікації (в першу чергу подача даних та оплата за надані послуги) надавач/споживач послуг (ЖКХ, опалення, водопостачання та водовідведення, постачання газу, теплової енергії та електроенергії тощо), телемедицина (eHealth), дистанційне навчання, сервіси з покупок та доставки товарів широкого вжитку і продуктів харчування із торгових мереж, банківська сфера (е-банкінг) тощо. Разом з рівнем цифровізації та глобалізації суспільства, відносин на рівні громадянин-суспільство-держава зростає кількість кіберзагроз, кіберінцидентів та кібернебезпек, які впливають на сталість функціонування комунікаційних мереж та інформаційно-телекомунікаційних систем. Отже, можна говорити про те, що «кожен

громадянин може розраховувати на власну безпеку в кіберпросторі», адже «кожен громадянин» повинен «усвідомити правила поведінки в кіберпросторі», бо тільки він сам відповідальний за захист, користуючись «корпоративною поштою, підключаючись до конференцій, обмінюючись файлами» [3] тощо. У зв'язку з цим виникає запит на стійкість та сталість функціонування створених інформаційних ресурсів, не зважаючи на зовнішні та внутрішні чинники впливу, в першу чергу, через зростання рівня кіберзагроз, кіберінцидентів та кібернебезпек. Оскільки «одними з найвразливіших місць віртуального світу є мобільний телефон із доступом до соціальних мереж, месенджерів, та десятків мобільних додатків часто невідомого походження, де люди з легкістю діляться приватною інформацією, яка, на перший погляд, не є критичною» [1]. Вказане відбувається у зв'язку зі збільшенням кількості громадян\споживачів послуг, які почали повсякденне використання цифрових технологій. Так, «загальна кількість комп'ютерних пристроїв, включаючи ноутбуки, настільні ПК, планшети і мобільні телефони, які знаходяться у використанні, в 2021 році досягне 6,2 млрд.штук» [2]. При цьому слід зважати на рівень кібер (комунікативної, комп'ютерної, ІТ, цифрової) компетентності та навичок тих осіб, які володіють та користуються таким кінцевим обладнанням. Особливістю сучасного світу є те, що у вирі новітніх технологій добре почуває себе наймолодше (цифрове) покоління, яке з народження має доступ до цифрових технологій) і у більшості випадків не отримує досвід від попередніх поколінь, а само їм його надає. Ось чому кіберкомпетеності та навички, хоча і відіграють важливу освітню роль, але головним запобіжником у сучасному цифровому світі проти кіберзагроз, кіберінцидентів та кібернебезпек визначається кібергігієна, яка при належному рівні виступає запобіжником для попередження кіберзлочинів через людський фактор (коли шахраї використовують соціальну інженерію та психологію впливу). Тим самим рівень кібергігієни впливає на «кількість Інтернет-шахрайств, фактів втручання в особистий простір, поширення неправдивих відомостей тощо нині набуває рис епідемії», коли нехтуються (свідомо чи через незнання) так званих «базових правил цифрової безпеки при роботі у світовій мережі та використанні різноманітних сервісів, що їх пропонують сучасні технології» [4]. Високий рівень кібергігієни сьогодні є запорукою безпеки людини (не тільки у кіберпросторі, а і на фізичному рівні), адже «хороша кібергігієна означає дотримання розумних щоденних практик щодо здоров'я та безпеки вашої інформації в Інтернеті» [5]. Тобто, основні рекомендації з кібергігієни повинні використовуватися людиною практично на підсвідомому рівні. Тільки так можна зменшити вплив кібершахраїв на людину в кіберпросторі. Але при цьому не треба забувати, що кібершахраї постійно збільшують арсенал, методи та інструменти впливу на людину з метою заволодіння її персональними даними, паролями та коштами, а тому підвищення рівнів кіберкомпетентності та кібергігієни повинно відбуватися регулярно на постійній основі. Якщо говорити про державних службовців, військових та працівників великих фірм та корпорацій, то для них проводяться відповідні курси підвищення кваліфікації, тренінги та навчання. Головна проблема постає серед інших верств населення, особливо старшого віку та тих людей, які не є постійними учасниками кіберкомунікацій. Ось тут і потрібна допомога з боку держави. Наприклад у цьому році Міністерство цифрової трансформації України та Координатор проектів ОБСЄ в Україні презентували новий освітній серіал «Основи кібергігієни», ознайомлення з яким дасть можливість «знати й застосовувати правила кібергігієни на роботі й у повсякденні; розуміти суть соціальної інженерії та психології впливу; безпечно користуватися браузером та загалом мережами Wi-Fi; розмежовувати використання особистої та службової поштових скриньок; розбиратися у використанні програмного забезпечення; вміти відповідально поширювати інформацію в соціальних мережах; опанувати правила безпечної роботи з мобільними пристроями; ознайомитися з роллю фізичної безпеки в кіберзахисті організації; розбиратися у видах маніпуляцій з інформацією у кіберсфері» [6]. Також необхідно враховувати потребу не тільки у навчанні, а і в практичній допомозі через створення відповідних «центрів надання кібердопомоги», якими необхідно охопити усю територію країни, адже на сьогодні відсутній механізм допомоги населенню в наданні практичної допомоги із кінцевим обладнанням (ноутбуки, настільні ПК, планшети і мобільні

телефони, смартфони, айфони) в частині антивірусних заходів та перевірки встановленого програмного забезпечення.

Підсумовуючи розгляд питань кібербезпеки та кібергігієни користувачів послуг на базі електронних комунікацій слід відзначити, що для збільшення ефективності протидії кібершахраїв необхідно виконання двох важливих умов, а саме: створення умов для постійного підвищення рівнів кібер компетеностей і навичок та формування кібервідповідальності через кібергігієну широких верств населення, в першу чергу старшого віку та тих, для кого цифрові технології не є основним засобом (знаряддям праці). Крім цього, формування кібербезпеки та кібергігієни необхідно починати формувати з раннього дитинства. Отже, для вжиття усіх необхідних заходів потрібно сформувати, затвердити та впровадити відповідний План заходів щодо розвитку кіберкомпетеностей та кібергігієни у населення (на коротку, середню та довгу перспективи) і чітко його дотримуватися та виконувати. Також необхідно створити мережу «центрів надання кібердопомоги», куди б міг звернутися будь-який громадянин та отримати допомогу. Адже населення залишається самим уразливим елементом системи стійкості та сталості функціонування мереж електронних комунікацій та послуг на їх основі.

СПИСОК ЛІТЕРАТУРИ:

1. Безпека в Інтернеті: найпростіші правила захисту даних. URL: https://www.bbc.com/ukrainian/blogs-51444737 (дата звернення: 01.06.2021).
2. Двойная мощность и новый ум. Каким будет последнее поколение смартфонов. URL: https://www.dsnews.ua/future/dvoynaya-moshchnost-i-novyy-um-kakim-budet-sleduyushchee-poslednee-pokolenie-smartfonov-16052021-425130 (дата звернення: 05.06.2021).
3. Жора В. Може, у кіберНАТО ми будемо швидше, ніж у реальному. URL: https://www.ukrinform.ua/rubric-technology/3249583-viktor-zora-zastupnik-golovi-derzavnoi-sluzbi-specialnogo-zvazku-ta-zahistu-informacii-ukraini.html90щ (дата звернення: 29.05.2021).
4. Кібергігієна – це важливо! URL: https://kpi.ua/2020-10-28 (дата звернення: 10.06.2021).
5. Кібергігієна … Що це? І 5 речей, які слід знати про це. URL: https://itech.co.ua/novyny/kiberhihiiena-shcho-tse-i-5-rechej-iaki-slid-znaty-pro-tse/ (дата звернення: 11.06.2021).
6. Мінцифри навчить держслужбовців основ кібергігієни. URL: https://www.kmu.gov.ua/news/mincifra-navchit-derzhsluzhbovciv-osnov-kibergigiyeni. (дата звернення: 29.05.2021).
7. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р. Урядовий кур'єр від 16.03.2021 № 50.

РОЗРОБЛЕННЯ ДЛЯ СФЕРИ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ІННОВАЦІЙНИХ СТАНДАРТІВ З ПІДГОТОВКИ ТА ВИКОРИСТАННЯ КАДРІВ

Мельник С.В.
ДНУ «Інститут освітньої аналітики» МОН України

Питання оновлення професійної та освітньої стандартизації з підготовки та використання кадрів в Україні набуло небувалої активності та розвитку. Це й не дивно, так як задекларований поступ України до європейського простору, запровадження стандартів НАТО тощо вимагають повного перезавантаження застарілих, неефективних, а часто-густо й шкідливих для економіки та суспільства систем управління та функціонування. Так, наприклад, починаючи із середини 2018 року в країні розроблено, затверджено та

запроваджено на практиці 171 професійний стандарт (документ нового покоління, який регулює вимоги до працівників через призму компетентностей та кваліфікацій) (https://www.me.gov.ua/Documents/Detail?lang=uk-UA&isSpecial=True&id=22469103-4e36-4d41-b1bf-288338b3c7fa&title=RestrProfesiinikhStandartiv). Сформований Перелік «регульованих» спеціальностей, запроваджена система визнання результатів неформального навчання, поширюється практика застосування дуальної форми освіти, затверджено більш як 200 стандартів вищої освіти очікуваними результатами навчання тощо, проводиться робота над новою версією Національного класифікатора України ДК 003 «Класифікатор професій» (далі – КП), яка базується на Міжнародній стандартній класифікації занять (ISCO-08) та Міжнародній класифікацій занять, навичок та кваліфікацій (ESCO) тощо.

Не стоїть осторонь від цих обнадійливих процесів і сфера захисту інформації та кібернетичної безпеки. Найближчим часом до КП будуть внесені суттєві зміни відповідного спрямування, а саме:

1. Будуть скасовані 2 посади:

2149.2 Професіонал із організації інформаційної безпеки

2149.2 Фахівець (сфера захисту інформації)

2. Будуть внесені такі 17 професій та посад:

2132.2 Розробник систем захисту інформації

2139.2 Адміністратор мереж і систем

2139.2 Аналітик загроз безпеки

2139.2 Аналітик захисту інформації та оцінки вразливостей

2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем

2139.2 Дізнавач (сфера кібербезпеки та захисту інформації)

2139.2 Експерт-криміналіст (сфера кібербезпеки та захисту інформації)

2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)

2139.2 Слідчий з кіберзлочинів

2139.2 Фахівець з криптографічного захисту інформації

2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології)

2139.2 Фахівець з підтримки інфраструктури кіберзахисту

2139.2 Фахівець з реагування на інциденти кібербезпеки

2139.2 Фахівець з тестування систем захисту інформації

2139.2 Фахівець з технічного захисту інформації

2139.2 Фахівець сфери захисту інформації

2359.2 Інструктор-методист з інформаційної безпеки та кібербезпеки.

Орієнтовний термін затвердження чергової (Зміна №10) до КП Міністерством економіки України – кінець липня 2021 року. Затвердження цих змін передбачає появу можливості у провайдерів вищої освіти розроблювати професійні стандарти та Галузеву рамку кваліфікацій сфери захисту інформації та кібернетичної безпеки, переглядати освітні стандарти та програми.

Крім того, Громадська організація «Асоціація спеціалістів кібербезпеки» виступила у ролі роботодавця-заявника професійного стандарту на кваліфікацію «Оператор з обробки інформації та програмного забезпечення», та працює над ним відповідно до встановлених процедур. Зрозуміло, що це не «університетська професійна кваліфікація», але це є великою нагодою отримати досвід з розроблення професійних стандартів та застосувати його за призначенням та потребою.

МІНІМІЗАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОСВІТНЬОМУ СЕРЕДОВИЩІ MOODLE

Бурбела О.О., Іванченко І.С., Кривокульська О.О.
Національний авіаційний університет

Одним із важливих напрямків глобалізації освітнього простору є використання засобів та систем дистанційної освіти (СДО), які дозволяють адекватно та гнучко реагувати на потреби суспільства та забезпечувати реалізацію конституційного права на освіту кожного громадянина. Зі збільшенням кількості та складності інформації зростає і кількість загроз інформаційної системи в цілому. Тому інформаційна безпека в системах дистанційного навчання на сьогодні є найвищим пріоритетом, ефективне рішення якого дозволить викладачам та студентам взаємодіяти один з одним, не турбуючись про збереження інформації [1].

Мета даного дослідження полягає у визначенні основних загроз інформаційної безпеки (ІБ), властивих всім віддаленим системам, зокрема СДО Moodle та підготовці рекомендацій для мінімізації цих загроз.

Для досягнення цілі дослідження потрібно вирішити наступні завдання:

1. Визначити основні загрози інформаційної безпеки систем дистанційного навчання.
2. Запропонувати рекомендації для мінімізації загроз ІБ з використанням програмних можливостей системи дистанційного навчання Moodle.

Аналіз статистики щодо порушень інформаційної безпеки та інцидентів від провідних компаній з інформаційної безпеки показує, що 82% інформаційних систем мають «вразливі» місця для несанкціонованого доступу (НСД) до ресурсів [2]. Особливо це стосується систем, що розповсюджуються в мережі, таких як СДО Moodle, архітектура яких винесена за периметр основної мережі навчального закладу і цілодобово доступна для користувачів глобальної мережі і може бути об’єктом цілеспрямованих атак.

Отже, процес визначення ІБ повинен включати всі засоби безпеки та сегменти в межах логічної та фізичної системи. Тому при створенні моделі загроз СДО Moodle слід виділити три основні структурні елементи:

1. Мережевий інтерфейс (SQL-ін'єкції, XSS-атаки, спам).
2. Сервер Moodle (підбір паролів та атаки на систему автентифікації користувачів, збільшення привілеїв, DDos-атаки).
3. База даних Moodle (викрадення персональних даних, НСД до баз даних).

Оскільки Moodle є веб-сайтом, інформація захищається двома способами:

- засобами хостингу, в якому розташована система;
- безпосередньо через саму систему.

Хости, на яких працює Moodle, зазвичай захищають інформацію за допомогою резервних серверів. Сучасний хостинг оснащений автоматичними системами захисту інформації від DDOS-атак та вбудованими антивірусними програмами, що захищають програмні файли від комп’ютерних вірусів.

Як програмний продукт, система управління навчанням Moodle є досить безпечною та захищеною від різних загроз, спаму та хакерських атак. З метою захисту інформаційних ресурсів у системі вона забезпечує [3]:

1) захист від SQL-ін'єкцій, XSS-атак, DDos-атак;
2) аутентифікацію користувачів для доступу до інформаційних ресурсів курсу;
3) обмеження доступу – кожному користувачеві надається відповідний рівень доступу до навчальних матеріалів системи;
4) резервне копіювання системи;

5) IP-блокування, яке виконує порівняння вхідних веб-адрес зі списком заблокованих IP-адрес;

6) захист HTTP;

7) вбудований антивірус Clam AV.

В якості рекомендацій щодо мінімізації загроз інформаційної безпеки засобами системи дистанційного навчання Moodle можна навести наступні.

1. Функція аутентифікації.

Налаштування складності пароля. В системі Moodle передбачено такі налаштування аутентифікації: пароль повинен мати принаймні 8 символів, включаючи хоча б 1 цифру, 1 літеру малого регістру, 1 літеру великого регістру та 1 спеціальний символ. Рекомендується встановити кількість послідовних однакових символів. Користувач може особисто змінити пароль не більше одного разу і з обов'язковим дотримання правил політики безпеки паролів.

Зашумлення паролів - це спосіб посилити захист, додавши до пароля випадковий набір символів (шум) перед обчисленням контрольної суми md5. Це ускладнює скидання пароля контрольної суми (чим довший набір випадкових символів, тим складніше це зробити).

2. Функція розмежування доступу. В системі Moodle передбачена можливість використання ролей. Дана функція реалізується шляхом створення та призначення різних ролей користувачам системи відповідно до їхньої ієрархії у закладі вищої освіти та надання кожній ролі належних прав доступу до інформації різної цінності.

Загалом, механізм розмежування доступу та грамотний підхід до надання прав користувачам мінімізує такі загрози ІБ, як спам, ризик конфіденційності, ризик атаки XSS та ризик втрати даних.

3. Функція резервного копіювання системи. Правильно налаштований механізм дозволяє захистити систему від втрати важливої інформації в результаті «відмови» операційних систем, шкідливого програмного забезпечення, різних кібератак, людського фактора тощо. Налаштування резервного копіювання Moodle дозволяють включати до копії: дані користувача, навчальну інформацію, журнали подій у основну резервну копію, а також налаштовувати розклад автоматичного створення резервної копії системи.

4. Функція IP-блокатор. Блокування IP-адрес, з яким надходить велика кількість запитів дозволяє підвищити захист системи Moodle від DDos-атак. У відповідні поля потрібно ввести IP-адреси, яким потрібно заблокувати доступ до СДО.

5. Функція «Захист HTTP». Система Moodle містить у своєму арсеналі ще один засіб захисту від НСД, а саме створення безпечного HTTP з'єднання для сторінок входу до системи. Налаштування дозволяє налаштовувати cookies, а також створювати список заблокованих хостів та дозволених портів.

6. Вбудований антивірус Clam AV. Вбудований антивірус Clam AV, який сканує всі завантажувані файли та навчальні матеріали. Плагін для роботи з цим антивірусом вже вбудований в ядро Moodle.

Отже, забезпечення інформаційної безпеки системи дистанційного навчання Moodle вимагає комплексного підходу до захисту освітніх інформаційних ресурсів, а представлені рекомендації дозволять підвищити працездатність системи та покращити ефективність заходів щодо збереження конфіденційності, цілісності та доступності інформації.

СПИСОК ЛІТЕРАТУРИ

1. Лужецький В. А. Інформаційна безпека: навч.посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – 240 с.

2. Positive Tecnologies. Актуальні кіберзагрози: 2020 року. [Електронний ресурс]. Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

3. Moodle Security [Електронний ресурс]. Режим доступу: https://docs.moodle.org/dev/Security.

ПІДХОДИ ДО ОЦІНКИ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Гончар С.Ф.[1], Комаров М.Ю.[2]

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

На сьогоднішній день не можна гарантувати повну захищеність будь-якої інформаційної системи, у тому числі об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури [1, 2].

У відповідності до [3], з метою оцінювання стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, і готовності підрозділів суб'єктів огляду, до повноважень яких належить забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури, захист державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, до ефективного і оперативного реагування на кіберзагрози, попередження, виявлення та захисту від кібератак і кіберінцидентів, ліквідації їх наслідків, відновлення функціонування об'єктів критичної інформаційної інфраструктури проводиться відповідний огляд. Одними із завдань огляду є проведення аналізу кіберстійкості критичної інформаційної інфраструктури, а також планування заходів щодо забезпечення кіберстійкості критичної інформаційної інфраструктури.

Найважливішим фактором забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури є створення системи управління кібербезпекою, яка повинна забезпечити стійке, живуче і безпечне функціонування об'єктів критичної інфраструктури; безпеку навколишнього середовища; захист інтересів особистості, суспільства і держави, а також споживачів послуг [4].

У [5] зазначається, що непередбачуваність, надзвичайна невизначеність та швидка еволюція потенційних кіберзагроз роблять зусилля з оцінки ризику неможливими для адекватного вирішення проблеми кібербезпеки для критично важливих інфраструктурних систем. З цієї причини традиційний підхід до зміцнення кіберсистем проти виявлених загроз виявився неможливим.

Питання забезпечення кіберстійкості відіграють ключову роль в подоланні ризиків кібербезпеки, кіберзагроз та невизначеностей, пов'язаних із кіберзагрозами. Рівень кіберстійкості інформаційної системи або організації визначається здатністю підтримувати або відновлювати свою базову функціональність після кібератаки. Інформаційна система з достатнім рівнем кіберстійкості здатна [6]:

- реагувати на регулярні та нерегулярні кіберзагрози надійним, гнучким (адаптивним) способом;
- відстежувати те, що відбувається, в тому числі власну продуктивність;
- прогнозувати ризики кібербезпеки, кібератаки, контрзаходи;
- здійснювати навчання на власному досвіді.

У роботі [7] кіберстійкість визначається як здатність процесу, бізнесу, організації передбачати, витримувати, відновлюватись і розвиватися в умовах деструктивних дій, кібератак на інформаційні ресурси, які являються критичними для функціонування. Також, у це визначення може бути включено здатність виявлення кіберзагроз. Приведені дослідження показують, що кіберстійкість дає можливість компаніям або інформаційним системам

проявляти стійкість проти змін сценарію кіберзагрози, маючи надійні та адаптовані способи протистояння кіберзагрозам.

Одним із основних принципів забезпечення кіберстійкості організації є те, що ця організація використовує свої активи (людей, інформацію, технології та обладнання) для підтримки конкретних оперативних місій або критичних служб [8]. Застосування цього принципу дає можливість зрозуміти можливості організації у виконанні, плануванні, управлінні, вимірюванні та визначенні практик та поведінки оперативної стійкості шляхом вивчення наступних десяти доменів [8]:

- керування активами;
- керування контролем;
- конфігурація та керування змінами;
- керування вразливістю;
- керування інцидентами;
- керування безперервністю обслуговування;
- керування ризиками;
- керування зовнішньою залежністю;
- навчання та обізнаність;
- ситуаційна обізнаність.

В роботі [2] визначено, що під кіберстійкістю розуміється здатність системи управління об'єкта критичної інформаційної інфраструктури виконувати свої функції в складних, різко змінюваних обставинах в умовах деструктивних кібервпливів. При оцінці кіберстійкості об'єктів критичної інформаційної інфраструктури як складових елементів критичної інфраструктури, яка функціонує у кіберпросторі, виникає ряд проблем, пов'язаних зі складністю об'єктів критичної інформаційної інфраструктури, складністю і різнорідністю зв'язків між ними і умовами спільного з противником використання ресурсів інформаційно-телекомунікаційної мережі загального користування.

В запропонованій в роботі [2] кіберстійкість представлена як інтегральний показник кіберзахищеності, кібернадійності та кіберживучості:

$$К_{ОКІІ}^{уп} = К_{ОКІІ}^{жив} * К_{ОКІІ}^{зах} * К_{ОКІІ}^{над}, \quad (1)$$

де:

$К_{ОКІІ}^{уп}$ – узагальнений показник кіберстійкості;

$К_{ОКІІ}^{жив}$ – кіберживучість об'єкта критичної інформаційної інфраструктури;

$К_{ОКІІ}^{зах}$ – кіберзахищеність об’єкта критичної інформаційної інфраструктури;

$К_{ОКІІ}^{над}$ – кібернадійність об’єкта критичної інформаційної інфраструктури,

Кіберживучість об'єкта критичної інформаційної інфраструктури трактується як здатність збереження його працездатності (виживання) в умовах виходу з ладу технічних засобів обробки інформації внаслідок деструктивних кібервпливів, тобто, по суті, – внесок кожного базового елемента об'єкта критичної інформаційної інфраструктури у виконання ним цільової функції. Математично кіберживучість трактується як ймовірність невиходу кінцевого стану системи із заданої безпечної області (тобто невиходу з ладу):

$$К_{ОКІІ}^{жив} = 1 - V_S, \quad (2)$$

де:

V_S – ймовірність виходу кінцевого стану системи із заданої безпечної області S (виходу з ладу).

Кіберзахищеність трактується як ймовірність забезпечення виконання цільової функції об'єкта критичної інформаційної інфраструктури із заданою якістю в умовах застосування «загальних» і цілеспрямованих деструктивних кібервпливів.

$$К_{ОКІІ}^{зах} = (1 - Р_{ЗКА}) * (1 - Р_{ЦКА}), \quad (3)$$

де:

$Р_{ЗКА}$ і $Р_{ЦКА}$ – ймовірності ураження технічних засобів обробки інформації, що входять до об’єкта критичної інформаційної інфраструктури, загальними ($Р_{ЗКА}$) та цілеспрямованими ($Р_{ЦКА}$) кібератаками.

Під кібернадійністю розуміється ймовірність забезпечення виконання цільової функції об'єкта критичної інформаційної інфраструктури протягом визначеного часового інтервалу в умовах виникнення різних подій (i = 1,…., N) – програмних та технічних відмов засобів об'єкта критичної інформаційної інфраструктури внаслідок деструктивних кібервпливів:

$$К_{ОКІІ}^{над} = \prod_{i=1}^{N} К_{ОКІІНАДі} (1 - Р_i). \quad (4)$$

З огляду на те, що узагальнений показник кіберстійкості трактується як добуток показників кіберживучості, кібернадійності та кіберзахищеності, його обчислення здійснюється за допомогою відповідного програмного застосунку.

Проведені дослідження показують, що кібербезпека включає технології, процеси та засоби контролю, призначені для захисту організацій та/або інформаційних систем від кіберзагроз у вигляді кібератак. Забезпечення кібербезпеки бередбачає зменшення ризику кібератак або наслідків, що мали б місце у результаті реалізації цих кібератак. Разом з тим, необхідно зазначити, що кіберстійкість являє собою більш широкий підхід, який охоплює кібербезпеку, управління безперервністю бізнесу. Кіберстійкість спрямована на захист від потенційних кібератак та забезпечення функціонування організації або інформаційної системи в штатному режимі після кібератаки.

СПИСОК ЛІТЕРАТУРИ

[1] Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури : монографія / С.Ф. Гончар. – Київ : «Альфа реклама», 2019. – 176с.

[2] Komarov, M., Honchar, S., & Dimitriieva, D. (2021). Дослідження проблеми кіберживучості об’єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 59-66. https://doi.org/10.32918/nrs.2021.1(89).07

[3] Постанова Кабінету Міністрів України «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» [Електронний ресурс] // № 1176 від 11 листопада 2020 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text.

[4] Комаров М.Ю. Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф. // Моделювання та інформаційні технології. – 2017. - №81. – С. 12-19.

[5] Igor Linkov. Fundamental Concepts of Cyber Resilience: Introduction and Overview [Електронний ресурс] / Igor Linkov, Alexander Kott, // Springer. – 2018. – Режим доступу до ресурсу: https://arxiv.org/ftp/arxiv/papers/1806/1806.02852.pdf

[6] Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation / Terje Aven // European Journal of Operational Research. – 2016. – Vol.253. – P. 1–13.

[7] Juan F. Carías, Saioa Arrizabalaga, Leire Labaka and Josune Hernantes. Cyber Resilience Progression Model / Juan F. Carías, Saioa Arrizabalaga, Leire Labaka and Josune Hernantes // Applied Scitnces. – 2020. – Vol.10(21), 7393.

[8] Carnegie Mellon University. Cyber Resilience Review (CRR). Department of Homeland Security 2016. Available online: https://www.us-cert.gov/ccubedvp/assessments (accessed on 7 March 2021).

ЕМУЛЯЦІЯ КІБЕРЗАГРОЗ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

Корченко А.О., Нагорний Ю.І., Бичков В.В.
Національний авіаційний університет

На сьогодні, одними із розповсюджених систем захисту інформації є системи виявлення кібератак та системи виявлення вторгнень (СВВ), останні з яких становлять особливий практичний та науковий інтерес [1, 2]. Також, функціональність сучасних систем виявлення та блокування вторгнень у значній мірі залежить від їх можливостей щодо виявлення нових кібератак у режимі реального часу. Для виявлення відповідних атакуючих дій використовуються спеціальні методи, моделі, засоби, програмне забезпечення і комплексні технічні рішення для СВВ, які можуть залишатись ефективними при появі нових або модифікованих кіберзагроз. Однак, як показує практика при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, відповідні засоби не завжди залишаються ефективними.

Отже, розробка засобів верифікації та проведення експериментальних досліджень відповідних технічних рішень, засобів і програмного забезпечення виявлення кібератак, зловживань та аномалій в інформаційних системах (ІС) для підтвердження адекватності їх роботи є актуальним науковим завданням.

Є низка робіт, таких як кортежна модель формування атакуючих середовищ, низка методів для виявлення аномальних станів, методологія побудови СВВ, а також структурна модель обчислювальної системи для створення засобів виявлення кібератак та її алгоритмічне і програмне забезпечення. Для її верифікації необхідний спеціалізований емулятор кіберзагроз, оскільки відомі не підтримують необхідні формати даних, що застосовуються у авторській розробці [3].

Виходячи з цього, метою роботи є розробка емулятора для проведення експериментального дослідження для підтвердження достовірності отриманих теоретичних положень, практичних результатів та адекватності роботи програмного модуля розробленої системи виявлення кібератак (СВК) [3], що дозволить удосконалити функціональні властивості сучасних СВВ для режиму реального часу.

Базуючись на структурній моделі СВК [3], здійснимо верифікацію відповідної програмної системи з метою підтвердження достовірності теоретичних положень наукових досліджень, проведених у роботі [3]. Для цього побудуємо структуру віртуальної мережі, за допомогою якої проведемо моделювання процесу реалізації різних типів загроз на ресурси ІС (РІС). Запропонована мережа складається з файл-сервера, СВК і шести клієнтів. Також, для реалізації атак за допомогою віртуальної мережі розроблено клієнт-серверний застосунок, що емулює роботу системи в режимі реального часу.

Система змоделює низку кібератак, для яких здійснені відповідні тестові розрахунки. Так, наприклад, з використанням [3] та отриманих експертних коефіцієнтів параметрів $(EC_{31}^{max},\ EC_{32}^{max})$ і кібератаки (EC_{3}^{CA}) визначимо умовний вираз з підмножини $\mathbf{DR_{3\,13}}$ [3] детекційного підсередовища ($\mathbf{DR_{SP}}$) для виявлення спуфінгу, що інтерпретується, як: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до значення еталону «Середнє» (з експертним коефіцієнтом *0,662*) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Мале» (з експертним коефіцієнтом *0,518*), то рівень аномального стану, породженого спуфінгом буде «Більш низький ніж високий» (з експертним коефіцієнтом кібератаки *0,59*)», що з урахуванням [3] можна записати, як

$$if\ \ (E(NUM_{SPKOP},3)\big|_{0,662} \wedge E(NUM_{SPKPOA},1)\big|_{0,518})\ then\ "БНВ"\big|_{0,59}.$$

Із застосованого еквівалентного представлення видно, що для виявлення кібератаки із підмножини $\mathbf{DR_{3\,13}}$ був застосований умовний вираз з ідентифікатором аномальності «Більш

низький ніж високий». Також, можна графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$) з ідентифікатором аномальності «Більш низький ніж високий», який інтерпретує аномалію у *2*-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i=P_3=P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA^{\tau_f}}$) в момент часу τ_f [3]. Відповідно до запропонованого прикладу видно, що при незначному (дещо вищого мінімального) рівні загроз програмна модель СВК ідентифікує аномальний стан, що може бути породжений кібератакою, як «Більш низький ніж високий». Це відповідає (з урахуванням експертних коефіцієнтів та коефіцієнта кібератаки) адекватній реакції СВК на незначний вплив загроз на РІС.

За результатами експерименту можна зробити висновок, що у всіх випадках модель СВК адекватно реагує на впливи атакуючого середовища. На основі такого типу програмних розробок можна удосконалювати сучасні СВВ за рахунок додаткової можливості динамічного (у режимі реального часу) контролю стану безпеки інформаційних систем відносно реалізованих кібератак та рівнів впливу різних типів загроз на РІС. Це, також, підтверджується наступними експериментальними даними, що адекватно відображають впливи атакуючого середовища.

За результатами застосування розробленого емулятора та проведеного експериментального дослідження що здійснювалось за допомогою розробленої віртуальної мережі [3], було проведене моделювання 2000 атак (з достатньо високим рівнем впливу на файл-сервер), кожна з яких виявлена за допомогою певного умовного виразу сформованого детекційного середовища, яке у розглянутому випадку складається з одного підсередовища ($\mathbf{DR_3=DR_{SP}}$). Вся множина модельованих кібератак була відповідно виявлена умовними виразами SP-середовища з ідентифікатором аномальності «Більш високий ніж низький», «Високий» та «Граничний», що входять у підмножини детекційних виразів $\mathbf{DR_{3\,13}}$, $\mathbf{DR_{3\,14}}$ та $\mathbf{DR_{3\,15}}$, на кожне з яких відповідно припало 32,35%, 45,5% та 22,15% реалізованих загроз на файл-сервер [3]. Проведені за допомогою емулятора експериментальні дослідження підтвердили достовірність основних теоретичних положень, практичних розробок та адекватність роботи програмного модуля СВК.

СПИСОК ЛІТЕРАТУРИ

1. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень», Захист інформації, Т.20, №4, С. 259-276, 2018.

2. І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, «Аналіз відкритих систем виявлення вторгнень», Безпека інформації. Т.24, №3, С. 201-216, 2018.

3. А. Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

КІБЕРБЕЗПЕКА ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ: ТЕХНІКО-ЮРИДИЧНИЙ АНАЛІЗ

Хлапонін Ю.І, Тернавська В. М.
Київський національний університет будівництва і архітектури.

Сучасний глобалізований світ активно розвивається у новій парадигмі інформаційного суспільства. Стрімкий розвиток національних економік та культури, плідна співпраця держав у сфері міжнародної безпеки стали можливими завдяки новим технологічним можливостям та поширенню мережі Інтернет. Зокрема, інтеграція сучасних інформаційних технологій створює умови для виникнення як локальних, так і національних кіберфізичних систем (КФС), що передбачають впровадження в процеси управління елементів штучного інтелекту [1, с. 78]. Кіберфізичні системи є ключовим інструментом забезпечення функціональності, надійності,

та безпеки критичних об'єктів та інфраструктур, зокрема аерокосмічних, енергетичних, транспортних, оборонних та ін. Найважливішою характеристикою критичних КФС є функціональна безпека, яка відповідно до міжнародних та національних стандартів визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та (або) його наслідки. Інформаційна безпека та її складова – кібербезпека значною мірою визначає функціональну безпеку КФС.

Виходячі з вищезазначеного, перед державою постають нові виклики, зумовлені можливостями сучасних інформаційних технологій, зокрема несанкціоноване поширення інформації, кібератаки на інформаційні бази даних національних систем управління, інформаційна війна тощо. Іншою проблемою є інтеграція нових технологій, таких як нові апаратні архітектури та нові комунікаційні протоколи, в існуючі сертифікаційні процеси Відповідно до Framework for Cyber-Physical Systems Release 1.0 May 2016 [2, с. 21].

Захист національних інтересів від реальних та потенційних загроз у кіберпросторі потребує застосування не лише організаційних, матеріальних, фінансових, технічних, але і правових інструментів. Однак, як слушно зауважують українські правознавці, Україна має недостатній потенціал щодо протидії загрозам її інформаційній безпеці та зміцненню в цілому національної безпеки, оскільки відсутня цілісність системи правового регулювання суспільних відносин у галузі протидії загрозам національним інтересам України в інформаційній сфері [3, с. 5]. Сьогодні необхідність удосконалення правового врегулювання вищезазначених питань вже зумовлюється навіть тим, що існує нагальна потреба визначення суверенітету держави у новому вимірі – інформаційному, та визначення меж реалізації інформаційного суверенітету держави [4, с. 40].

Аналіз національного інформаційного законодавства свідчить про відсутність системного підходу нашого законодавця до вирішення питання належного правового врегулювання інформаційної сфери. Річ у тім, що частина нормативно-правових актів безнадійно застаріла, а тому не може належним чином врегульовувати нові суспільні явища у сфері інформаційних технологій, а нові потрібні акти ще не прийняті з різних причин. Крім того, недотримання правил нормотворчості та юридичної техніки призводить до колізій правових норм, результатом чого є наявність у законодавстві України трьох різних визначень поняття «інформація», трьох визначень поняття «захист інформації». Натомість поняття «інформаційна безпека» не визначено ні Законом України «Про інформацію» від 02.10.1992 р. № 2657-XII, ні Законом України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII. Відповідно застосовується поняття «кібербезпека», що містить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII [5]. Необхідно зазначити, що поняття "кібербезпека", яке міститься в даному Законі, є невід'ємною та необхідною складовою кіберфізичних систем як стан безпечного, надійного, стійкого їх функціонування з урахуванням вимог конфіденційності. Натомість даний Закон не дає визначення поняття кіберфізичних систем. Виходячи з вищезазначеного, автори пропонують доповнити Закон наступним визначенням даного поняття: «кіберфізична система (КФС) – це інтелектуальна система, що включає інженерно взаємодіючі мережі фізичних та обчислювальних компонентів».

Вирішенням проблеми неналежного нормативно-правового регулювання суспільних відносин в інформаційній сфері може стати, на думку фахівців, запровадження правових режимів у сфері кібербезпеки. Так, на думку В. В. Бєлєвцевої, належно розроблена та втілена в життя категорія правового режиму кіберпростору могла б усунути надмірну розшарованість правового регулювання, більш чітко та послідовно визначити суб'єктів досліджуваних правовідносин та порядок їх взаємодії, юридичні гарантії забезпечення прав людини, форми, методи діяльності контролюючих суб'єктів, заходи юридичної відповідальності [6, с. 108-109]. Своєю чергою Н. Ф. Казакова та інші спеціалісти з питань комп'ютерних та інформаційно-вимірювальних технологій наголошують, що для машинних і когнітивних інтерфейсів, повинен бути створений новий правовий режим функціонування, який визначить правила реагування на конфліктні ситуації між суб'єктами міжмашинної взаємодії [1, с. 78].

Таким чином, удосконалення механізму правового регулювання інформаційної сфери шляхом приведення національного інформаційного законодавства, що включає в себе нормативно-правові та нормативно-технічні акти, до стандартів міжнародного права та права ЄС є безпосередньо питанням національної безпеки, що передбачає як захист державного суверенітету, так і дотримання прав людини.

СПИСОК ЛІТЕРАТУРИ

1. Казакова Н.Ф., Щербина Ю.В., Фразе-Фразенко О.О. Проблеми безпеки сучасних кіберфізичних систем. Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.). – Одеса: Одеський державний університет внутрішніх справ, 2017. С. 77-78. URL : http://dspace.oduvs.edu.ua/handle/123456789/500

2. Framework for Cyber-Physical Systems Release 1.0 May 2016 Cyber Physical Systems Public Working Group. URL : www.nist.gov

3. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. Правова інформатика. 2009. № 4 (24). С. 5-12.

4. Солодка О. М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. Інформація і право. 2020. № 4 (35). С. 39-46.

5. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

6. Бєлєвцева В.В. До питання застосування правових режимів забезпечення кібербезпеки в Україні. Інформація і право. 2020. № 4 (35). С. 106-112.

МОБИЛЬНАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА МОНИТОРИНГА КАЧЕСТВА ВОЗДУХА

Ахметов Б.С.,[1] Лахно В.А.,[2] Блозва А.И.,[2] Абуова А. К.,[3] Шалабаева М. Х.[3]

[1]Казахский Национальный педагогический университет имени Абая, Алматы, Казахстан Национальный университет биоресурсов и природопользования Украины

[2]Национальный университет биоресурсов и природопользования Украины

[3]Казахский университет путей сообщения, Алматы, Казахстан

Спроектированная мобильная автоматизированная система мониторинга качества воздуха (МАСМКВ), которая может быть использована в местах чрезвычайных происшествий (техногенных аварий), например, на железнодорожном транспорте (ЖДТ).

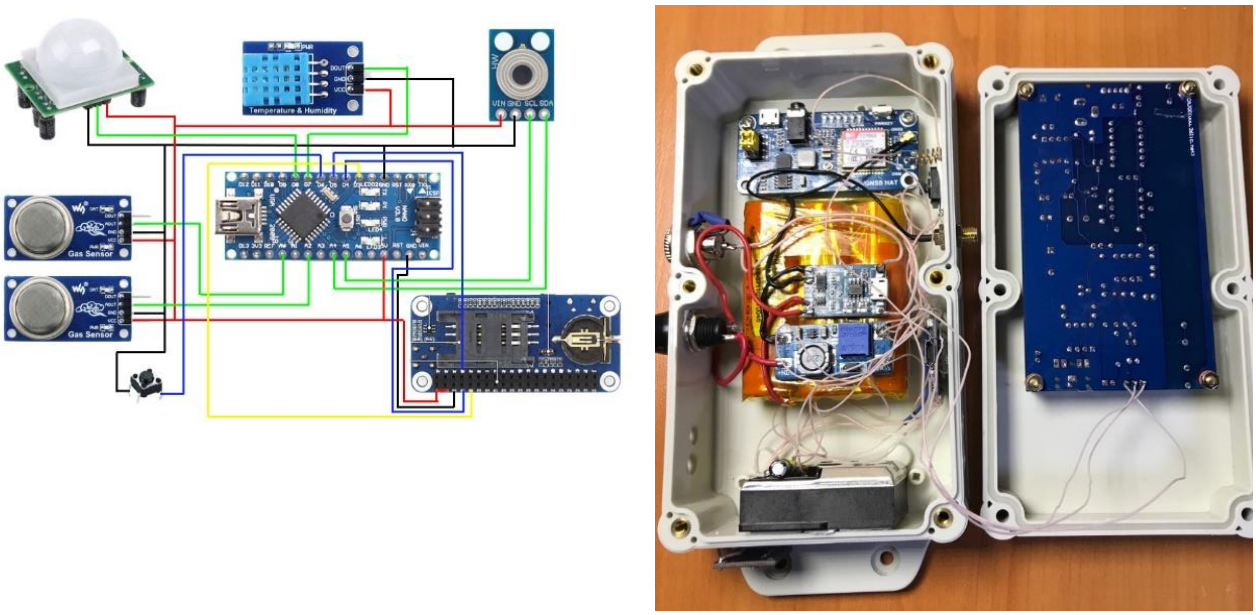
На основании проведенных исследований были получены такие результаты:

Спроектирована и реализована система мониторинга качества воздуха на инфраструктурных объектах ЖДТ. Система (или МАСМКВ), см. рис. 1 состоит из двух основных частей: единого сервера обработки данных и устройств сбора информации. Передатчик построен на базе микроконтроллера ATmega328. Для компонентных устройств МАСМКВ работа которых зависит от WiFi, использован передатчик на базе микроконтроллера ESP8266, что обеспечивает стабильную связь по стандарту 802.11n. Данный стандарт является основным протоколом передачи данных между устройствами сбора данных об окружающей среде и сервером MQTT.

Показано, что преимуществами такого выбора протокола 802.11n являются: простота и использовании, простое администрирование, низкая нагрузка на канал связи, работа в условиях постоянной потери связи или других проблем на линии, отсутствие ограничений на формат передаваемого контента.

В реализованном МАСМКВ сервер обработки данных получает информацию через протокол MQTT со всех устройств о состоянии каждого датчика и местонахождение устройства в месте ЖД аварии, сопровождавшихся загрязнением окружающей среды. Все

данные с определенной периодичностью записываются в базу данных на сервере в соответствующем формате с временными метками. Для доступа к хранимым данным используется WEB-интерфейс, что позволяет администрировать МАСМКВ из всех устройств, которые имеют веб-браузер.



а) б)

Рис. 1. Схема и общий вид мобильной автоматизированной системы мониторинга качества воздуха

Система мониторинга (МАСМКВ) успешно протестирована ЖД Украины и Казахстана на стабильность и скорость работы. Во время тестирования выполнена модификация приборов передачи данных. Так в частности, модифицированы система электропитания за счет применения дополнительных высокочастотных фильтров. Работа веб приложения МАСМКВ протестирована на разных системах виртуализации и с разным количеством предоставленных вычислительных ресурсов.

Выполнена программная реализация формального описания действий аварийных подразделений как процессов функционирования системы массового обслуживания без временных ограничений на платформе технологии ADO.net. Установлены количественные соотношения между интенсивностью воздействия опасных факторов ЖД АС, времени прибытия, развертывания и производительности действий ликвидационных подразделений и эффективностью выполнения ликвидационных работ, связанных с минимизацией ущерба для окружающей среды от опасных грузов, перевозимых ЖДТ.

Результатами компьютерного моделирования с помощью разработанного приложения показано, что существенное уменьшение негативного влияния последствий ЖД АС на окружающую среду возможно при сокращении срока проведения ликвидационных работ, а также при уменьшении времени сосредоточения подразделений и применения сил и средств необходимой производительности. А увеличение времени сосредоточения требует увеличения в разы производительности таких сил и средств. В ходе имитационных вычислительных экспериментов на ЭВМ установлено, что если средства ликвидации последствий ЖД АС не соответствуют ее характеру и/или крайне малопродуктивны, то даже при их своевременном сосредоточении на месте ликвидации, они не будут эффективными. Или же, даже если средства ликвидации достаточно эффективны, но сосредоточение их на месте возникновения этой ситуации произошло с опозданием, то они также не дадут эффекта.

Вывод необходимой информации в МАСМКВ происходит с помощью веб-интерфейса, который также является системой администрирования приборов с датчиками, см. рис. 2.

Рис. 2. Страница отображения дополнительной информации с графиками о состоянии воздуха в месте ЖД аварии

Серверное программное обеспечение выполняет одну из важнейших функций в системе мониторинга качества воздуха в местах ЖД аварий. Сервер получает данные с устройств в районе аварии, фильтрует и сохраняет информацию с датчиков и предоставляет доступ к просмотру хранимой информации в виде графиков. Для выполнения данных функций сервера нужно предоставлять достаточное количество вычислительных ресурсов.

СПИСОК ЛІТЕРАТУРИ

1. Грига, В., Сачовський, А., & Мандзюк, В. Специализированная система измерения качества воздуха на базе ESP32. С. 12.

2. Arsyad, N. A., Syarif, S., Ahmad, M., & As'ad, S. (2020). Breast milk volume using portable double pump microcontroller Arduino Nano. *Enfermeria clinica*, *30*, 555-558.

МОДЕЛІ ОПТИМАЛЬНОГО ФУНКЦІОНУВАННЯ БЕЗПЕКИ ВІДДАЛЕНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Хохлачова Ю.Є., Аль-Далваш А.
Національний авіаційний університет

Сьогодні методи і засоби несанкціонованого доступу та інформації в сфері з широким застосуванням ПЕОМ, взаємодіючих через локальні і глобальні мережі, набули такої популярності, що нерідко саме поняття «захист інформації» застосовується позитивно в сенсі захисту інформації, що обробляється в автоматизованих системах (АС). Однак, як вважають фахівці, захист інформації (ЗІ) в мережах слід виділити в окремий канал, рівноцінний іншим технічним каналам витоку інформації [1].

Звичайно, в певному сенсі витік інформації з інформаційних мереж також виникає згодом недосконалості програмно-апаратних рішень, реалізованих в АС. Але, тим не менше, користуючись подібними вадами в архітектурі АС та інформаційних мережах (ІС), зловмисник може використовувати їх ресурси і процеси для проведення несанкціонованого доступу (НСД) до інформації.

Кількість методів і засобів несанкціонованого доступу до інформації з АС і ІС при віддаленому доступі значно ширше і досить сильно залежить від використовуваної операційної системи (ОС), налаштування параметрів безпеки і т.п. Як не парадоксально, але найбільш ефективними (з деякими обмовився) при віддаленому доступі є системи і мережі, що працюють під управлінням операційних систем, які найбільш вразливі при локальному доступі. Це пов'язано з тим, що в них практично відсутні розвинені засоби, що надаються собою зовнішні по відношенню до ядра таких систем модулі, слабо інтегровані з іншими компонентами подібних найпростіших ОС. Тому, якщо використовувати АС, що працює під управлінням такої ОС, то найпростіші правила безпеки (наприклад, ненадання доступу по мережі до файлів і папок свого комп'ютера), його система має високий ступінь стійкості до несанкціонованого доступу [1.2.3].

Слід зазначити, що за рідкісним винятком більшість сучасних ОС під час налаштування параметрів, прийнятих за замовчуванням, не є безпечними з точки зору функціонування в інформаційних мережах [3].

Основна частина. При побудові моделі безпечного доступу до інформації упор робиться на зіставлення наявних заборонених засобів (активних і регулярно використаних) і ступеня жорсткості політики безпеки в АС і ІС щодо контролю віддаленого доступу (в загальному випадку контроль доступу на увазі збереження цілісності інформації, доступності та недопущення факту ознайомлення з нею в процесі передачі, обробки та зберігання в самій інформаційної мережі) і дотримання конфіденційності інформації при її передачі по інформаційних мереж. При цьому враховується статистика випадків несанкціонованого доступу в ІС, що мають місце раніше. Нижче наведена таблиця показників, якими оперує модель віддаленого доступу.

Модель безпеки Internet-з'єднання

Мережа Internet - це багатогранна і розвивається, живе своїм життям, і в той же час є невід'ємною від нашого життя інформаційне середовище, в якій існують методи і засоби, що дозволяють вирішувати завдання інформації в земному середовищі.

Основне значення будь-якої мережі (в тому числі і Internet) полягає в обов'язку доставити необхідну інформацію користувачеві. Причому, системи захисту інформації в мережі повинні сприяти ефективному виконанню основної функції ІС Internet сучасному обміну інформацією. Інакше кажучи, не ІС робиться під систему захисту, а система захисту допомагає ІС (в тому числі і Internet) і є допоміжним (але дуже вірним) компонентом. З цього випливає, що перш ніж переходити до забезпечення безпеки мережі, необхідно визначитися з моделлю самої ІС. [4].

Перш за все необхідно визначитися з погрозами самій мережі. Це можливість здійснення

дії, що направляється проти об'єкта захисту (мережі), що проявляється в небезпеці спотворень і втрат інформації. Необхідно обумовить, що мова йде не про всю інформації, а тільки про ту її частини, яка, на думку користувача, має певну цінність або підлягає захисту відповідно до домену [5].

Необхідно також враховувати, що джерело загроз безпеки може перебувати як усередині мережі, та й зовні. Зіставлення загроз інформації в ІС і групи методів їх протидії дозволило вирішити, такими способами які загрози найдоцільніше нейтралізувати, а також визначити раціональне співвідношення груп методів при розподілі коштів, виділених на забезпечення безпеки інформації в ІС.

Можна виділити цілий ряд причин, за якими потрібно забезпечити інформаційну безпеку ІС, а також Internet:

По-перше, різноманітні функції забезпечення інформаційної безпеки досить сильно інтегровані в існуючі технології побудови ІС і систем;

По-друге, сучасні інформаційні технології немислимі без активного користування публічних сервісів, представлених ІС і в першу чергу, Internet. З цієї причини ІС необхідно призначити той чи інший спосіб до відкритих мереж, що можна робити тільки при забезпеченні безпеки з'єднання.

По-третє, грамотно побудована і реалізована інформаційна безпека може істотно розширити функціональні можливості ІС;

• Побудова системи віддаленого захищеного доступу користувачів до інформаційних ресурсів ІС;

• Використання Internet-комунікацій для передачі інформації між різними користувачами і т.д. [4,5].

Тому модель безпечного Internet-з'єднання відповідно до ступеня загроз і ризиків локальної ІС має на увазі наявність набору захисних засобів, сумарний ваговий коефіцієнт, який згідно табл.1 знаходиться в межах: низький ризик - 0,3: середній ризик - 4 10, високий ризик - більше 10.

Таблиця 1

Сумарні вагові коефіцієнти

K_{TRN}	K_{JAV}	K_{CERT}	K_{IMPRT}	K_{AVIR}	$R_{SEC,MAN}$	$R_{FW,USG}$
Низький – 0 Середній – 1 Високий – 3	Так – 1 Ні – 0	Так – 1 Ні – 0	Низький – 0 Середній – 2 Високий – 4	Низький – 0 Середній – 3 Високий – 5	Так – 5 Ні – 0	Низький – 1 Середній – 4 Високий – 7

Висновки

Опис моделі дозволяє оптимально регламентувати доступ в локальну ІС із зовнішніх мереж з точки зору безпеки інформації, визначити чисельні значення ймовірностей несанкціонованого доступу для даного вище з'єднання, вибрати на основі отриманих даних оптимальний набір захисних механізмів. При оцінці ймовірностей успішних закономірних дій приймається до уваги як перелік існуючих засобів захисту, так і даних про спроби несанкціонованих дій за час функціонування локальної мережі, що дозволяє отримати більш точні імовірнісні значення. Моделі можуть застосовуватися як на стадії проектування мережі з можливістю віддаленого доступу, так і в процесі її експлуатації.

СПИСОК ЛІТЕРАТУРИ

1. Ленков С.В. Методи і засоби захисту інформації. Том 1. Несанкціоноване здобування інформації / Ленков С.В., Перегудов Д.А., Хорошко В.О. - К: Арій, 2008. – 464с.

2. Домарев В.В. Захист інформації і безпека комп'ютерних систем / В. В. Домарев - К: Вид. «Дія Софт», 1999. – 480с.

3. Соколов О.В. Захист інформації в розподілених нормативних мережах і системах / А.В.

Соколов, В.Ф. Шаньчін - М: ДМК Пресс, 2002 – 656с.
4. Vacca J. Internet Security Secrets - Chicago: IDG Books Worldwide, Inc., 1996. - 505p.
5. Федотов О.В. механізми можливих атак в мережі Internet / Е.В. Федотов // Захист інформації. Зб. науч. Праць НАУ - К: НАУ, 2001. – С. .30-43.

ОЦІНЮВАННЯ КІБЕРЗАХИСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Хохлачова Ю.Є., Аясрах А.
Національний авіаційний університет

Процес випровадження нових інформаційних технологій в усі сфери життя сучасного суспільства, що вступає в інформаційний період, неможливий без рішення ниток інформаційної та кібербезпеки в різних сферах діяльності суспільства . Широкомасштабне використання обчислювальної техніки та телекомунікаційних систем, перехід до безпаперової технології, збільшення об'ємів оброблювальної інформації й розширення кола користувачів, приводить до якісно нових, можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем (ІС), до її високої вразливості. В сучасних умовах захист інформації в цілому й кіберзахист в інформаційних системах зокрема стає все більш складною проблемою.

Масове створення впровадження і експлуатація ІС привели до виникнення нових проблем в сфері безпеки інформації. І це закономірно.

Потреби в забезпеченні безпеки пов'язані з тим, що існує множина суб'єктів і структур, які зацікавлені в чужій інформації та готові платити за це високу ціну.

В таких умовах все більше розповсюджується аксіома, що захист інформації повинен по своїм характеристикам відповідати масштабам загроз. Відхилення від цього правила приведе до додаткових збитків. Для кожної ІС мається оптимальний рівень захищеності, який необхідно постійно підтримувати[1].

Немає сумнівів, що захист, критично важливих для ІС масивів повинен відповідати сучасним нормативним документам. Застосовуються високовартісні технічні засоби та впроводжуються суворо регламентовані заходи та методи. Однак немає відповіді на найважливіше питання – наскільки рішення які запропоновуються або реалізовуються, дійсно відповідають вимогам.

Тому для запобігання втрати або пошкодження інформації використовуються системи захисту інформації, що являють собою комплекс засобів і методів які перешкоджають несанкціонованому доступу до інформації.

Основним напрямком пошуку ефективних шляхів захисту є підвищення системності підходу до самої проблеми захисту інформації. Поняття системності інтерпретується перш за все в тому сенсі, що захист інформації полягає не просто у створені відповідних механізмів, а являє собою регулярний процес, який здійснюється на всіх етапах життєвого циклу обробки даних при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи та заходи, які використовуються для захисту інформації, об'єднуються в єдиний цілісний механізм – систему захисту, що повинна забезпечувати захист не тільки від зловмисників, але й від некомпетентних або недостатньо підготовлених користувачів та персоналу.

Тому при проектуванні або модифікації ІС однією з найважливіших проблем є проблема оцінювання якості захисту(кіберзахисту). Ця проблема повинна вирішуватися системно, тому що довільне переважання одного з аспектів захисту приводить до недооцінки інших, що врешті може суттєво зменшити рівень захисту (кіберахисту) системи загалом [1,2]. Як не дивно, але в багатьох випадках зловмисники діють більш системно ніж користувачі ІС, особливо коли усілякі доробки системи реалізуються власними силами, а не первісними проектами.

Виходячи з цього розглянемо основні компоненти, які найчастіше зазнають активних втручань в роботу ІС оскільки системний аналіз можливих втручань у роботу цих систем і дає можливість оцінити дійсний рівень захисту тієї чи іншої системи.

Основними компонентами, які найчастіше зазнають активних втручань в роботу ІС є наступні (рис.1):

-користувачі системи (1);
-моделі довірчих відношень (2);
-проектні рішення та їх реалізації (3);
-архітектура системи (4);
-обладнання (5);
-програмні засоби відновлення після збоїв (6);
-засоби захисту (7);

Одним з найбільш розповсюджених видів атаки на ІС з боку зловмисника, який зазвичай прекрасно знає психологію користувача, є атака з врахуванням «людського» чинника. Тобто, якщо аналіз алгоритмів потребує багато місяців кропітної щоденної праці, то атака з врахуванням фактору реального користувача може виявитися значно більш швидкою та ефективною. Це особливо відчутно, якщо ще й ІС спроектовано недостатньо добре, та «кодекс поведінки» користувача або не існує, або дотримання його положень не контролюється з боку адміністратора системи [2].

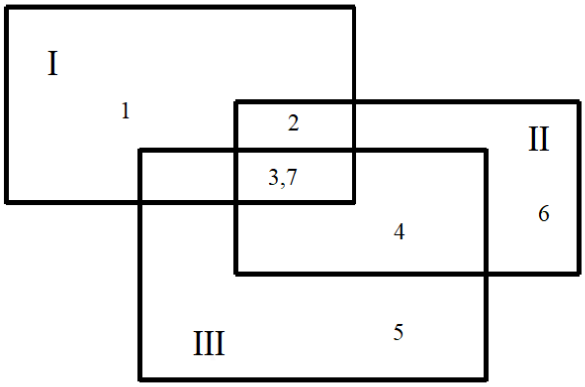


Рис.1 Основні компоненти та ланки можливого (=) втручання в роботу ІС

Часто користувачі не приділяють необхідної уваги перевірці електронного підпису. Секретні паролі часто повторно використовуються в ІС. Звичайно, навіть системи, які мають потужну систему захисту, не в змозі ліквідувати наслідки «людського» фактору, але вони можуть зводити їх до мінімуму.

Необхідно забезпечити чітко регламентовану з паролями та іншими засобами ідентифікації користувачів, виконувати мінімальні вимоги до надійності паролів.

Моделі довірчих відношень в системі повинні бути чіткими. Тобто, якщо модель довірчих відношень не чітка, то в процесі розгортання в інформаційної бази випадково внести деякі непродумані зміни, після чого нормальне функціонування систем безпеки буде порушено.

Крім цього, слід враховувати, що процес захисту пов’язаний з конфліктом між стороною, що забезпечує безпеку (кібербезпеку) інформації та стороною яка бажає незаконним шляхом отримати її. Для аналізу такого конфлікту краще за все підходить теорія ігор, так нам вона дозволяє моделювати дії обох сторін. Теорія ігор – це теорія математичних моделей прийняття оптимальних рішень в умовах конфліктів. Вона дозволяє отримати стратегію раціональної поведінки для отримання максимального виграшу чи максимальної ймовірності виграшу [3].

В залежності від цінності інформації до системи захисту(кіберзахисту) можуть ставитись різні вимоги. При цьому можливі дві принципово різні ситуації, що обумовлюють необхідність вирішення відповідно першої чи другої. Перша ситуація передбачає, що інформація є комерційною або некомерційною таємницею. В даному випадку наслідком втрати інформації для власника будуть економічні втрати, що можна оцінити кількісно. Тобто, задача оптимізації полягає в тому, щоб при певному розмірі затрат на систему захисту забезпечити максимальний рівень захисту.

Друга ситуація виникає, коли інформація складає державну таємницю, і неможливо оцінити вартість затрат від її втрати. При цьому система захисту (кіберзахисту) має забезпечити необхідний рівень безпеки (кібербезпеки) інформації, а оптимізація полягає в мінімізації затрат ресурсів для забезпечення безпеки та необхідного рівня захисту.

Не потрібно цілком і повністю покладатись на захищеність апаратних та програмних засобів. Багато користувачів занадто довіряються захищеності програмних засобів замість апаратних засобів. Передбачається, що ПЕОМ абсолютно безпечний. Рано або пізно в процесі забезпечення функціонування комп'ютера, проникає програма яка підбирає паролі, зчитує незашифрований текст або якимось іншим чином втручається в роботу ІС та систем захисту. Розробникам ІС, що функціонують у інформаційних мережах, варто потурбуватися про безпеку мережевих протоколів. Уразливість ПЕОМ, залучених до Internet, багаторазово зростає. В особливо рідких випадках можлива побудова двох не пов'язаних між собою мереж.

Дуже часто система проектується в розрахунку на одну модель довірливих відносин, а в процес реалізації функціонує зовсім інша. Прийняті в процесі проектуванні рішення ігноруються користувачем після передачі йому системи.

Існує багато способів подолання захисних систем, які пов'язані з моделями довірчих відношень усередині системи. Насамперед, варто виявити зв'язок між окремими компонентами систем, усвідомити обмеження та механізми реалізації схем довірчих відношень.

Тому необхідно визначити критерії оцінювання захищеності ІС. В результаті аналізу характеристик (спроектованих та реальних) ІС та систем захисту визначаємо наступі характеристики:

l – кількість компонентів ІС.

m – кількість захисник механізмів, що використовуються тестовій ІС.

n – кількість загроз несанкціонованих дій до компонентів ІС.

$\mu_{ik} \in [0,1]$, **i**=1,2,…, **n** – коефіцієнт небезпеки загроз несанкціонованих дій(НСД) для кожного компонента ІС, k=1, l,…,l

$\gamma_{ijk} \in [0,1]$ **j**=1,2,…, **m** – коефіцієнт ефективності використання механізму захисту **j** від **i** загрози НСД до компонентів ІС.

a_{ik} – затрати на реалізацію загроз на компонентах ІС.

b_{jk} – вартість засобів захисту на компонентах ІС.

C_k – інформаційна вартість компонента ІС.

Рішення про відповідність ІС вимогам захищеності від НСД приймаються на основі порівняння результатів розрахованого шляху захищеності з вимогам, що визначені в програмі випробовування.

Дана модель розрахунку інформаційної захищеності може бути використана для розрахунку узагальненого (пізнання) захищеності ІС, використовуючи поля загроз, характерних для інформаційної моделі ІС.

Таким чином, у програмі електронної пошти може використовуватися супернадійний алгоритм шифрування повідомлень, але якщо ключі не сертифіковані джерелом, що заслуговує довіри, і сертифікація не може бути підтверджена в реальному часі, безпека системи залишається під сумнівом.

Якісні моделі довірчих відношень продовжують працювати навіть у тому випадку, якщо окремі компоненти ІС або систем захисту відмовляють.

Проектні рішення та реалізації слід перевіряти на наявність типових «дір» в захисті та усунути їх. При чому багато систем підводять помилки в реалізації рішень. Деякі реалізації проектних рішень не гарантують, що зашифрувавши текст, вони знищать оригінал. У інших системах для попередження втрати інформації у випадку системного збою використовують тимчасові файли, у цьому випадку на них можуть залишатися окремі фрагменти незашифрованого тексту. Усе це приклади дір у системах НСД, котрі часто використовуються зловмисниками.

У сучасних крипто системах термін життя ключів обмежуються максимально коротким проміжком часу. Процедура відновлення дозволяє продовжити життя ключа вже після того, як від нього відмовилися. Використовувані для відновлення ключів бази даних, само по собі є джерелом небезпеки, і їхня архітектура повинна бути вивірена з особливою старанністю.

Тому, проектні рішення повинні орієнтуватися на чітку регламентацію роботи з метою забезпечення необхідного рівня захисту системи загалом.

У випадку використання різних стандартів в одному середовищі, необхідно забезпечити чітку взаємодію між ними. Тому в системі слід звернути увагу на точки взаємодії між протоколами обміну даних та методами шифрування, які окремо один від одного є надійними[5].

Деякі системи шифрування, що використовують пов’язані ключі, можуть бути зламані, навіть якщо кожен ключ окремо надійний.

Іноді в зловмисників з’являється можливість скористатися оберненою сумісністю різноманітних версій програмного забезпечення. Як правило, у кожному новому варіанті програмного забезпечення розробники намагаються усунути «діри», що були в старому. А (=) застосувати протокол старої, незахищеної версії.

Надійність – важлива складова комплексної системи безпеки, але не варто вважати, що захищають лише від зловмисних дій і НСД. Деякі системи мають так зване «кільце безпеки», що складається з апаратних засобів підвищеної стійкості до несанкціонованого проникнення [6]. Розробники виходять із припущення, що архітектура системи усередині цього кільця надійно захищена від НСД. Більшість подібних технологій не працюють, а інструменти для захисту безупинно удосконалюються.

Слід уникати використання алгоритмів шифрування власної розробки або випадкових та коротких ключів. Це пов’язано з тим, що, як правило, розкрити відомі алгоритми шифрування вдається лише у виняткових випадках. Якщо розробник робить ставку на власні методи, шанси ламання підвищуються багаторазово і незнання секрету алгоритму не є особливою перешкодою. Тому у ІС повинні використовуватись якісні генератори випадкових чисел щодо роботи по створенню ключів. В багатьох випадках генератор випадкових чисел залежить від особливостей апаратного а програмного забезпечення [7]. Сама система шифрування може бути виконана на високому рівні, але якщо генератор випадкових чисел видає ключі, що можна вгадати, захист руйнується.

Логічно навести багато прикладів помилок у системах шифрування: програми повторно генерують особливі випадкові значення, алгоритми шифрованого підпису не в змозі забезпечити контроль за переданими параметрами, хеш-функції відкривають те, що повинні захищати. У протокол шифрування вносяться не передбачені розробниками зміни. Користувачі люблять «оптимізувати» наявні засоби, зводячи нанівець захист(кіберзахист) інформаційної системи.

Надійна система захисту (кіберзахисту), повинна самостійно виявляти несанкціоновані операції. При чому, один з основних принципів проектування подібних систем полягання в знанні того, що рано або пізно атаки зловмисника увінчаються успіхом, а тому дуже важливо своєчасно розпізнати такий напад та прийняти всі необхідні заходи для того щоб мінімізувати збитки.

Важливою є наявність засобів та організаційних процедур для якнайшвидшого відновлення працездатності ушкодженої в наслідок атаки системи. Тобто, необхідно генерувати нові пари ключів, замінити протокол, припинити використання розкритих

зловмисником засобів, виключити із системи вузли, до яких зловмиснику вдалося одержати доступ і т.д. Нажаль, багато програмних засобів не займаються збором потрібної інформації, не контролюють ситуацію і не в змозі надійно захистити дані від змін.

Всі події, що дозволяють встановити факт нападу або несанкціонованих дій, повинні реєструватися. Тобто, система безпеки (кібербезпеки) повинна бути комплексною та не обмежуватися рамками засобів шифрування та спеціальним обладнанням.

Якщо зловмисникам вдасться перебороти перші оборонні рубежі, повинні спрацьовувати додаткові механізми захисту. Потрібно постаратися максимально ускладнити задачу супротивника та зробити її рішення не вигідним з економічної точки зору.

СПИСОК ЛІТЕРАТУРИ:

1. Кобозєва А.А. Аналіз захищеності інформаційних систем/А.А. Кобозєва, І.О. Мочалін, В.О. Хорошко – ІС: Вид. ДУІКТ, 2010. – 316с.
2. Козюра В.Д. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах/В.Д. Козюра, Ю.М. Ткач, М.Є. Шелест та ін. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 144с.
3. Мулен Е. Теорія ігор/ Е. Мулен – М:Мир, - 1985. – 199с.
4. Петросян Л.А. Теорія ігор/Л.А. Петросян, Н.А. Зінкевич, Е.А. Семеня – Высшая школа менеджмента 1998. – 301с.
5. Скотт Бармен Розробка правил інформаційної безпеки / Бармен Скотт – М:ІД «Вільямс», 2002. – 208с.
6. Brailovskyi N., Khoroshko V., Khokhlacheva Y., Ayasrah Ahmad Evolution of the Level of Cyber Security of Information//Scientific and Practical Cyber Security Journal, vol.3, №3, 2019. – p. 18-24

ЗАСОБИ ОЦІНЮВАННЯ ШКОДИ ВІД ВТРАТИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУОМ

Лозова І.Л., Біскупський А.В., Горожанова А.О.
Національний авіаційний університет

Втрата інформації є серйозною проблемою для підприємств будь-якого розміру – втрата даних означає втрату часу та грошей на відновлення системи або відновлення інформації, яка є важливою для компанії. Звіт IBM «Про вартість порушення даних» виявив, що середня загальна вартість втрати інформації становить 3,86 мільйона доларів і стрімко рухається вгору [3].

Для адекватного процесу оцінки ризиків інформаційної безпеки та для відповідності законодавчим вимогам, компанії необхідно правильно і точно оцінити усю критичну інформацію. Для побудови системи захисту інформації, слід розуміти її цінність та оцінити можливі збитки від втрати інформації з обмеженим доступом (ІзОД).

Метою даної роботи є дослідження засобів та інструментів оцінки шкоди від втрати ІзОД на їх адаптивність і застосовність для різних потреб користувача (компанії).

Проведено аналіз існуючих засобів оцінки збитків від втрати ІзОД за наступними критеріями: не має обмежень від напрямку/галузі Компанії та інформації, що циркулює всередині неї; забезпечує якісну, кількісну або якісну та кількісну оцінку; розроблений для мікро, малих, середніх або великих компаній; враховує вимоги міжнародного та/або вітчизняного законодавства; метод є інтегрованим в систему оцінки ризиків (інструмент); враховує визначену цінність інформаційних активів; при оцінці враховує тип ОС серверу, де розміщується ІзОД.

Калькулятор IBM, Калькулятор NetDiligence. Дані засоби дозволяють провести кількісну оцінку втрати ІзОД в компанії не залежно від галузі в якій вона знаходиться, розроблені з урахуванням найкращих міжнародних практик та стандартів GDPR, PCI DSS, HIPPA та розраховані на компанії малого та середнього розмірів. Калькулятори представлені на веб-ресурсах, складаються з набору питань різного типу відповіді, після чого одразу видають результат оцінки збитків [3, 6].

Для розрахунку шкоди від втрати ІзОД, користувач має відповісти на наступні 7 запитань: 1) Скільки записів було втрачено? 2) Який тип даних було втрачено? 3) Це перше порушення організації? 4) Чи зберігалися дані в централізованій системі / місці? 5) Чи можливе використання цих даних для шахрайства? 6) Чи очікується колективний позов на компанію через втрату даних? 7) Чи наразі ваша організація охоплює порушення даних?

Давши відповіді на всі запитання, користувач отримує розраховану вартість втрати ІзОД в валюті – долар США. Для прикладу, якщо компанія втратить 20 даних з обмеженим доступом, які можливо будуть використані шахраями, але таке порушення є першим для компанії, та на разі колективного позову не очікується, то середня вартість запису складатиме – $9,010, а загальні збитки оцінюються в $180,203 (Рис.1.).

Калькулятор At-bay (Рис.2). Працює за тим самим принципом, що й калькулятори IBM та NetDiligence проте разом з тим, враховує вимоги американського стандарту CCPA.

Калькулятор Cloud Ready. Працює за тим самим принципом, що й калькулятори IBM та NetDiligence, однак враховує тип ОС (лише Windows та Linux) серверів, на яких розміщена ІзОД. Після вдалого проходження опитування, результат відправляються на e-mail пошту користувача.

CRAMM. Методологія CRAMM пропонує використання автоматизованих засобів для управління ризиками. Даний засіб дозволяє провести якісну та кількісну оцінки втрати ІзОД в компанії не залежно від галузі в якій вона знаходиться, розроблений з урахуванням найкращих міжнародних практик та підходить як для малих так і великих компаній. Засіб інтегрований в інструментальну систему оцінки ризиків та враховує визначену цінність інформації. Оцінка проводиться за десятибальною шкалою, причому критеріїв оцінки може бути кілька – фінансові втрати, втрати репутації тощо. В описах CRAMM як приклад наводиться така шкала оцінки за критерієм «Фінансові втрати, пов'язані з відновленням ресурсів» [7] (див. табл. 1).

Для оцінки можливого збитку CRAMM рекомендує використовувати такі параметри: шкода репутації організації; порушення чинного законодавства; збиток для здоров'я персоналу; збитки, пов'язані з розголошенням персональних даних окремих осіб; фінансові втрати від розголошення інформації; фінансові втрати, пов'язані з відновленням ресурсів; втрати, пов'язані з неможливістю виконання зобов'язань; дезорганізація діяльності.

Метод експертної оцінки. Метод експертних оцінок є частиною теорії прийняття рішень, а саме експертне оцінювання – процедура отримання оцінки проблеми на основі думки фахівців з метою подальшого прийняття рішення [8]. Даний метод дозволяє провести якісну оцінку втрати ІзОД в компанії не залежно від галузі в якій вона знаходиться, розроблений з урахуванням найкращих міжнародних практик та розрахований на велику та зрілу компанію. Метод передбачає залучення внутрішніх та/або зовнішніх фахівців та враховує визначену цінність інформації.

Адитивна модель оцінки цінності інформації. Припустимо, що є інформація, яка представлена у вигляді кінцевої множини елементів, і завдання полягає в оцінці даної інформації в грошовому еквіваленті. При використанні адитивної моделі визначення цінності базується на експертних оцінках компонент даної інформації, і при об'єктивності грошових оцінок її компонент підраховується шукана величина – їх сума в грошовому еквіваленті [1]. Основна проблема полягає в тому, що кількісна оцінка компонент інформації часто оцінюється необ'єктивно, навіть при її оцінці висококваліфікованими фахівцями – причина полягає в неоднорідності компонент інформації в цілому [2]. Для вирішення цієї проблеми прийнято використовувати ієрархічну відносну шкалу, яка представляє собою лінійний порядок, за допомогою якого порівнюються окремі компоненти інформації, що захищається за цінністю

одна щодо іншої. Даний метод дозволяє провести якісну оцінку втрати ІзОД в компанії не залежно від галузі в якій вона знаходиться, розроблений з урахуванням найкращих міжнародних практик та розрахований на велику та зрілу компанію. Метод передбачає залучення внутрішніх та/або зовнішніх фахівців.

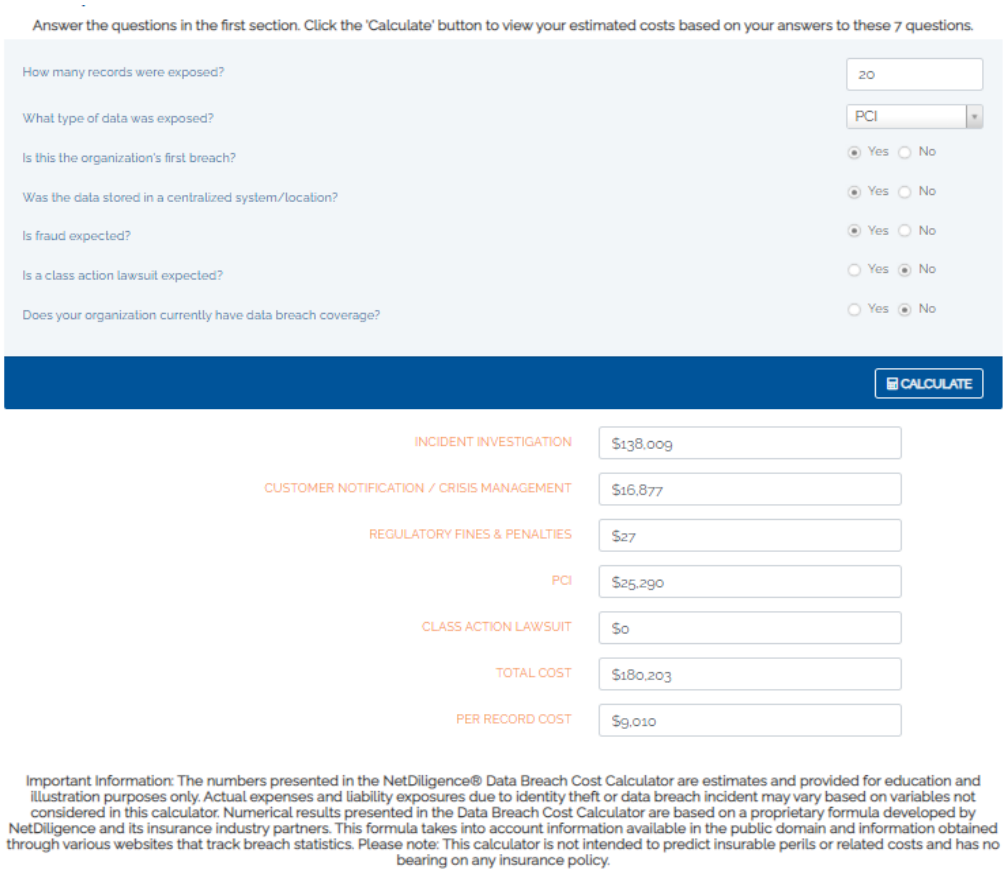


Рис.1. Приклад розрахунку збитків від втрати ІзОД калькулятором NetDiligence [5]

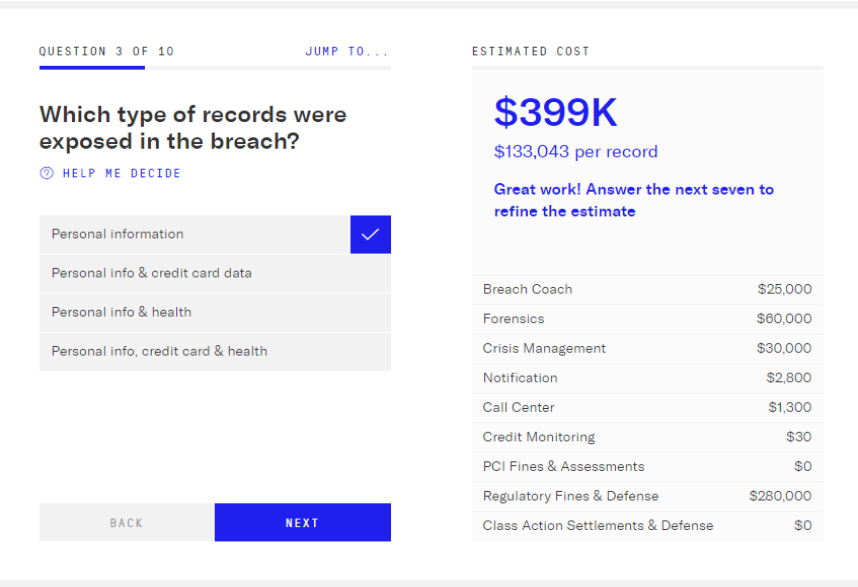


Рис. 2. Приклад розрахунку збитків від втрати ІзОД калькулятором At-bay [4]

Таблиця 1

Шкала оцінки CRAMM

Шкала балів	Величина фінансових втрат
2 бали	менше $ 1000
6 балів	від $ 1000 до $ 10 000
8 балів	від $ 10 000 до $ 100 000
10 балів	понад $ 100 000

FRAP. Методологія FRAP (Facilitated Risk Analysis Process) є відносно спрощеним способом оцінки ризиків, з фокусом тільки на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки. Даний засіб дозволяє провести якісну оцінку втрати ІзОД в компанії не залежно від галузі в якій вона знаходиться, розроблений з урахуванням найкращих міжнародних практик та розрахований на малу або середню компанію. Засіб інтегрований в інструментальну систему оцінки ризиків та враховує визначену цінність інформації. Оцінка проводиться для ймовірності виникнення загрози і шкоди від неї за наступними шкалами (див. табл. 2).

Таблиця 2

Шкала оцінки FRAP

Імовірність (Probability):	Збиток (Impact) – міра величини втрат або шкоди, що завдається:
• Висока (High Probability) – дуже ймовірно, що загроза реалізується протягом наступного року;	• Високий (High Impact): зупинка критично важливих бізнес-підрозділів, яка призводить до істотного збитку для бізнесу, втрати іміджу або неотримання істотного прибутку;
• Середня (Medium Probability) – можливо загроза реалізується протягом наступного року;	• Середній (Medium Impact): короткочасне переривання роботи критичних процесів або систем, що призводить до обмежених фінансових втрат в одному бізнес-підрозділі;
• Низька (Low Probability) – малоймовірно, що загроза реалізується протягом наступного року.	• Низький (Low Impact): перерва в роботі, не викликає відчутних фінансових втрат.

Відповідно до проведеного дослідження переваг та недоліків існуючих засобів оцінювання шкоди від втрати ІзОД, представимо порівняльний аналіз вказаних засобів (табл. 3).

Таблиця 3

Порівняльний аналіз засобів оцінювання шкоди від втрати інформації з обмеженим доступом

Параметри	Калькулятор IBM, Калькулятор NetDiligence	Калькулятор At-bay	Калькулятор Cloud Ready	CRAMM	Метод експертної оцінки	Адитивна модель оцінки цінності інформації	FRAP
Не має обмежень від напрямку/галузі Компанії та інформації, що циркулює всередині неї	+	+	+	+	+	+	+
Забезпечує якісну оцінку				+	+	+	+

Забезпечує кількісну оцінку	+	+	+	+			
Розроблений для мікро та малих компаній	+	+	+	+			+
Розроблений для середніх компаній	+	+	+	+	+	+	
Розроблений для великих компаній				+	+	+	
Враховує вимоги європейського стандарту GDPR	+	+	+				
Враховує вимоги американського стандарту CCPA		+					
Враховує вимоги вітчизняного законодавства	+	+	+	+	+	+	+
Засіб інтегрований в систему оцінки ризиків (інструмент)				+			+
Враховує визначену цінність інформаційних активів		+		+	+		+
При оцінці враховує тип ОС серверу, де розміщується ІзОД		+	+				

Отже, було проаналізовано методи оцінювання шкоди від втрати ІзОД, їх переваги та застосовність під потреби компанії. За допомогою даного аналізу, вдалось продемонструвати широкий спектр видів засобів оцінювання збитків від втрати ІзОД та виокремити їх головні характеристики.

СПИСОК ЛІТЕРАТУРИ

1. Грушо А. А., Тимонина Е. Е. Ценность информации // Теоретические основы защиты информации. — М.: Издательство Агентства «Яхтсмен», 1996. — С. 52-55.
2. Симонов С. Современные технологии анализа рисков в информационных системах // PCWEEK. — 2001. — № 37.
3. Cost of a Data Breach Report // IBM Security. – 2020. – С. 76.
4. How much will a data breach cost my company? [Електронний ресурс] – Режим доступу до ресурсу: https://keeprisk.at-bay.com/svc/data_breach_calculator.
5. NetDiligence® Mini Data Breach Cost Calculator [Електронний ресурс] – Режим доступу до ресурсу: https://eriskhub.com/mini-dbcc.
6. Data Breach Cost Calculators [Електронний ресурс] – Режим доступу до ресурсу: https://iapp.org/resources/article/data-breach-cost-calculators/.
7. Никуленко Е.Д., Губенко Н.Е. Анализ модели для оценки потерь, связанных с реализацией угроз и уязвимостей для информационных систем // Сборник материалов II всеукраинской научно-технической конференции студентов, аспирантов и молодых ученных «Информационные управляющие системы и компьютерный мониторинг». Донецк: ДонНТУ, 2013 Т.1. С. 260-263.
8. Методи експертних оцінок: теорія, методологія, напрямки використання : монографія / Б. Є. Грабовецький. — Вінниця : ВНТУ, 2010. — 171 с. Г 75 ISBN 966-641-359-1

ВЕРИФІКАЦІЯ ІНТЕРНЕТ-КОНТЕНТУ НА ОЗНАКИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Лозова І.Л., Хохлачова Ю.Є., Пустовий І.О.
Національний авіаційний університет

Щодня в мережі з’являється велика кількість різного контенту: тисячі коментарів від користувачів соціальних мереж та форумів на різні теми, наприклад, такі як політика, спорт,

розваги, робота, розвиток технологій, міжнародні відносини тощо. І кожна точка зору, відгук та рейтинг має великий вплив на соціальну думку та поведінку. Це піднімає питання про аналіз емоційного забарвлення тексту.

Метою даної роботи є дослідження існуючих методів та засобів верифікації інтернет-контенту на наявність інформаційно-психологічного впливу та розробка власного програмного засобу, завданням якого є підвищення точності результату аналізу тональності текстів.

Аналіз тональності тексту (сентимент-аналіз, англ. Sentiment analysis [1]) – клас методів контент-аналізу в комп'ютерній лінгвістиці, призначений для автоматизованого виявлення в текстах емоційно забарвленої лексики і емоційної оцінки авторів (думок) по відношенню до об'єктів, мова про які йде в тексті [2].

Існують різні алгоритми, які можна застосувати в моделях аналізу настроїв, залежно від того, скільки даних потрібно проаналізувати, і наскільки точною повинна бути модель. Алгоритми аналізу настроїв поділяються на три групи:

1. *На основі правил*: ці системи автоматично виконують аналіз настроїв на основі набору правил, які створені вручну. Зазвичай система, заснована на правилах, використовує набір створених людиною правил, щоб ідентифікувати суб’єктивність, полярність або предмет думки. Ці правила можуть включати різні методи, які розроблені в обчислювальній лінгвістиці, такі як: стеммінг , токенізація, позначення та розбір частини мови та лексикони (тобто списки слів та виразів) [3].

Системи, засновані на правилах, дуже наївні, оскільки не враховують, як слова поєднуються в послідовності.

2. *Автоматичні методи*, на відміну від систем, заснованих на правилах, покладаються не на правила, створені вручну, а на техніки машинного навчання. Завдання аналізу настроїв, як правило, моделюється як проблема класифікації, за допомогою якої класифікатор подається текстом і повертає категорію, наприклад позитивну, негативну або нейтральну [4].

Штучні нейронні мережі (ШНМ, англ. artificial neural networks, ANN), або конективістські системи (англ. connectionist systems) – це обчислювальні системи, натхнені біологічними нейронними мережами, що складають мозок тварин. Такі системи навчаються задач (поступально покращують свою продуктивність на них), розглядаючи приклади, загалом без спеціального програмування під задачу [5].

3. *Гібридні системи* поєднують як заснований на правилах, так і автоматичний підходи.

Проведено дослідження існуючих програмних засобів для верифікації інтернет-контенту на наявність інформаційно-психологічних впливів а саме аналізу тональності текстів. На основі проведеного аналізу складено порівняльну таблицю програмних засобів.

Awario. Програмний продукт Awario від білоруської компанії BelPrime призначений для відстеження та аналізу згадки ключових слів в Інтернеті. Онлайн-сервіс Awario надає ряд аналітичних інструментів для обробки отриманих даних, що дозволяють проводити такі дослідження: відстеження трендів; аналіз тональності; аналіз впливу і виявлення центрів формування думки [6].

Brand24. Надійний та доступний засіб моніторингу засобів масової інформації, який допомагає керувати репутацією в Інтернеті, відстежувати та оцінювати маркетингові кампанії, відстежувати своїх конкурентів, отримувати відгуки клієнтів, робити соціальні продажі тощо [7].

Twitter SA. Twitter дозволяє компаніям особисто взаємодіяти зі споживачами. Обробка згадувань бренду в Twitter за допомогою аналізу настроїв дозволяє компаніям зрозуміти свою аудиторію, не відставати від того, що говорять про їх бренд і конкурентів і відкривати нові тенденції в галузі [8]. Цей програмний застосунок в більшості використовується як API та дає змогу з легкістю інтегрувати цей інструмент в свою систему.

Sentiment Analyzer. Sentiment Analyzer використовує «обчислювальну лінгвістику та видобуток тексту», щоб визначити почуття фрагмента тексту. Потім він складає та порівнює свої результати, щоб отримати загальний бал. Це робить його корисним інструментом для компаній, які прагнуть швидко розшифрувати намір заплутаної реакції клієнта [9]. Аналізатор

настрою пройшов навчання за допомогою колекції понад 8000 зразків письма та стенограм усних бесід, які з'являються в Американському національному корпусі (ANC). ANC містить зразки написання з найрізноманітніших жанрів та доменів [10].

Таблиця 1

Порівняння інструментів аналізу тональності текстів

Параметри	**Awario**	**Brand24**	**Twitter SA**	**Sentiment Analyzer**
Цінова модель	Starter – $24/міс Pro - $89/міс Enterprise - $249/міс	Plus - $49/міс Premium - $99/міс Max - $199/міс	Безкоштовно, поставляється як API	Безкоштовно
Мова	Будь-яка	90 мов	Англійська, французька	Англійська
Підтримка пристроїв	Веб-орієнтований, хмарне рішення	Хмарне рішення, підтримується на всіх пристроях	Application programming interface (API), можна інтегрувати в будь-який додаток	Веб-орієнтований
Метод класифікації	На основі правил, мішок слів (bag of words)	На основі правил, мішок слів (bag of words)	Наївний Байєсівський класифікатор + мішок слів (bag of words)	На основі словників
Додаткові можливості	Сповіщення на електронну пошту, звіти у форматі PDF та HTML	Мобільні сповіщення, звіти у форматі PDF, Excel, електронної пошти та інфографіки	Можна змінити параметри розробки, наприклад додати свою мову і т.д.	–

В процесі проведеного дослідження було виявлено *недоліки існуючих методів та засобів* для аналізу тональності а саме:

– потреба великого обсягу тренувальних даних;
– складне навчання – в основному потрібно доповнювати базу чи змінювати набір;
– неможливість визначити сарказм, контрастність, гумор – це основна проблема аналізу тональності.

Розроблено програмний застосунок на основі вдосконаленого методу аналізу тональності текстів за рахунок використання детального набору вхідних даних нейронної мережі та заздалегідь тренованої Word2Vec моделі векторизації та токенізації текстів.

В якості набору даних для нейронної мережі ми використовуємо набір користувацьких рецензій та відгуків з ресурсу IMDb (Internet Movie Database). Набір даних IMDb має формат *.csv та складається з 50000 оглядів фільмів англійською мовою (25000 для навчання та 25000 для тестування), а двійкова ціль для кожного огляду вказує, що вона є негативною (0) або позитивною (1). Вхідні дані проходять обробку та доводяться до оптимальної для використання функціями структури.

Далі дані розділяються на дані для тренування та для тестування. Наступним кроком йде впровадження заздалегідь тренованої Word2Vec моделі. З її допомогою ми додаємо токени до основних вхідних даних для більш ефективного навчання. Цією ж моделлю ми векторизуємо текстову інформацію в наборах для тренування та тестування, готуємо масиви даних для обробки нейронною мережею.

Будуємо нейронну мережу. Параметри нейронної мережі: розмір шару векторного уявлення = 50; розмір батчу = 300; темп навчання = 0.1; кількість кроків навчання = 1000; Dropout = 0.2; прихований розмір long short-term memory (LSTM) шару (кількість LSTM-модулів в блоці) = 50. Після побудови мережі тренуємо її. Параметри тренування: кількість епох = 5; розмір батчу = 34. Після тренування підлаштовуємо модель під наші початкові значення та тестуємо.

Під час розробки програмного засобу були визначені певні програмні та апаратні вимоги для правильного функціонування програмного засобу:

Програмні вимоги: Python версії 3.7; середовище розробки PyCharm Community Edition; Tensorflow версії 2.0 або вище; Інтерпретатор Miniconda з встановленим Tensorflow GPU.

Апаратні вимоги: Процесор: Intel або AMD що має мінімум 4 ядра та 8 потоків; ОЗП: мінімум 8 Гб (рекомендовано 16 Гб і більше); GPU: рекомендовано мати NVIDIA з підтримкою Compute Unified Device Architecture (CUDA) Drivers; 1.5 Гб вільного місця на диску для файлів програми.

Програмний застосунок розроблено шляхом використання рекурентної нейронної мережі (РНМ) з LSTM блоками, вхідні дані якої попередньо обробляються моделлю Word2Vec.

Алгоритм роботи складається з 10 основних етапів: 1. Імпорт бібліотек; 2. Введення даних; 3. Очищення набору даних; 4. Розділення набору даних на тренувальний та тестувальний; 5. Завантаження заздалегідь навченої Word2Vec моделі; 6. Векторизація текстів; 7. Вкладення токенів; 8. Визначення РНМ з LSTM блоками; 9. Тренування РНМ; 10. Тестування РНМ.

Було проведено експериментальне дослідження розробленого застосунку, що довело працездатність методу аналізу тональності текстів. Також проведено порівняння з засобом аналізу тональності текстів Twitter SA, що показало на 10,8% точніший результат розробленого програмного засобу проти існуючого.

Розроблений програмний застосунок аналізу тональності текстів може використовуватися для прогнозування ринку цінних паперів, обчислення індексу суб'єктивного благополуччя, прогнозувати результати виборів, оцінювати реакцію на якісь події або новини. Для бізнесу цей застосунок корисний тим, що з його допомогою можна аналізувати свій імідж серед користувачів та конкурентів, відслідковувати відгуки про продукти та для визначення цільової аудиторії. Недоліками розробленого програмного застосунку є відсутність користувацького інтерфейсу та високі апаратні вимоги для функціонування. Ці недоліки стануть направленням для удосконалення програмного засобу.

СПИСОК ЛІТЕРАТУРИ

1. Bo Pang, Lillian Lee. Opinion Mining and Sentiment Analysis // Foundations and Trends in Information Retrieval – 2008. – No. 2. – P. 1-135.
2. Аналіз тональності тексту [Електронний ресурс] // Wikimedia Foundation, Inc.. – 2017. – Режим доступу до ресурсу: https://cutt.ly/enYLYfc.
3. Sentiment Analysis: A Definitive Guide [Електронний ресурс] // MonkeyLearn – Режим доступу до ресурсу: https://monkeylearn.com/sentiment-analysis/.
4. Sentiment analysis methods for understanding large-scale texts. // EPJ Data Sci. – 2017. – №6. – С. 28.
5. Штучна нейронна мережа [Електронний ресурс] // Wikimedia Foundation, Inc.. – 2018. – Режим доступу до ресурсу: https://cutt.ly/onYLIce.
6. Awario: Описание, Функции и Интерфейс [Електронний ресурс] // Soware – Режим доступу до ресурсу: https://soware.ru/products/awario.
7. Brand24 Reviews & Product Details [Електронний ресурс] // G2 – Режим доступу до ресурсу: https://www.g2.com/products/brand24/reviews#details.
8. How to Do Twitter Sentiment Analysis with Machine Learning [Електронний ресурс] // MonkeyLearn – Режим доступу до ресурсу: https://monkeylearn.com/blog/sentiment-analysis-of-twitter/.

9. The Best 12 Sentiment Analysis Tools in 2021 [Електронний ресурс] // HubSpot. – 2021. – Режим доступу до ресурсу: https://blog.hubspot.com/service/sentiment-analysis-tools.
10. Free Sentiment Analyzer [Електронний ресурс] // LinksDanielSoper.com – Режим доступу до ресурсу: https://www.danielsoper.com/sentimentanalysis/default.aspx.

БЕЗПЕЧНИЙ КРИПТОВАЛЮТНИЙ ГАМАНЕЦЬ

Бистрова Б.В., Вишневська Н.С., Тараненко К.О.
Національний авіаційний університет

Дивлячись на реалії, не можна заперечувати, що криптовалюти та технологія блокчейну додають потенційний генератор рентабельності інвестицій та можливість керувати всією грошовою інформацією. Криптовалюти та технології блокчейну представляють простий спосіб отримати велику віддачу та підвищену ліквідність.

Найбільша загроза безпеці від роботи криптографічних систем – це дії які можуть скомпрометувати систему. Тому актуальним питанням є розробка засобів, що відповідають критеріям безпеки користувача, таким як: безпека зберігання приватного ключа, безпечне збереження даних до бази даних, безпека запитів до бази даних, двофакторна афтентифікація користувача, офлайн підпис транзакції приватним ключем.

Метою роботи є дослідження існуючих типів криптогаманців та існуючих випадків втрати даних; розробка програмного забезпечення, яке за допомогою одностороннього шифрування та шифруванням кодовим словом, безпечно зберігає дані користувача та забезпечує функцію здійснення криптовалютних платежів.

Дослідження типів криптовалютних гаманців. Криптовалютні гаманці можна розділити на дві основні категорії: холодні та гарячі гаманці. Різницею між двома з них є те, що для гарячих гаманців необхідне підключення до Інтернету, а для холодних гаманців – ні. Користувачі зазвичай використовують гарячий гаманець для того, щоб купити щось в Інтернеті і отримати невелику суму грошей для цієї мети, тоді як холодний гаманець – це просто як сховище в банку для зберігання різних видів цифрових цінностей [1].

На сьогоднішній день немає такого криптогаманця, який би відповідав всім вимогам та забезпечував належний захист персональних та приватних даних користувача. В наявних гаманцях ключ не шифрується та зберігається в первісному вигляді в базах даних. Персональні дані не хешуються та при зломі баз даних зловмиснику доступні всі дані користувачів.

Порівняння типів криптогаманців. Було проаналізовано існуючі гаманці, а саме паперові, апаратні, програмні, мобільні та інтернет гаманці щодо їх функціональних можливостей, та ризику втрати приватних даних, з метою отримання загального розуміння типів криптогаманців, їх переваг та недоліків. Проведено відповідне оцінювання (1 бал – найнижчий показник, 5 – найвищий), що зображено в табл. 1 [2].

Таблиця 1

Порівняння типів криптогаманців

	Паперові	Апаратні	Програмні	Мобільні	Інтернет
Зручність у використанні	1	3	4	5	4
Безпека приватного ключа	5	5	4	3	2
Доступ користувача до власного приватного ключа	5	4	4	3	2
Швидкість здійснення транзакції	1	3	5	5	5
Невразливість до вірусних програм	5	5	4	1	2
Невразливість на проникнення мережі	5	5	2	2	1

З проведеного аналізу можна зробити висновки, що підвищена безпека у гаманцях здійснюється за рахунок зручності використання, та навпаки. Наразі, є проблема знаходження «золотої» середини.

Відповідно до мети роботи було досліджено випадки витоку даних користувачів, втрати активів та їх причини [3] (Табл. 2.).

Таблиця 2

Дослідження випадків витоку даних та їх причини

Криптовалютні сервіси	Причина	Наслідок
Tether	Неналежне зберігання приватних та секретних даних.	Приватний ключ «центрального» гаманця було втрачено.
BitHumb	Використання входу до систему лише за допомогою пароля. Шифрування персональних даних не було.	Втрата персональної інформації користувачів.
BitGo	Вразливість проникнення у мережу та отримати віддалений доступ до серверів. Не шифрування даних.	Ключі для підпису транзакцій було втрачено.
AllCrypt	Слабкий захист на проникнення у мережу.	Незашифровані приватні ключі бази даних було втрачено.
Inputs.io	Використання старих електронних адрес без приєднаного номеру телефону.	Був отриманий доступ до бази даних користувачів.
BitcoinCentral	Використання сумнівного хостинг-провайдера, який не використовував 2FA автентифікацію.	Активи та приватні ключі було втрачено.
BitFloor	Використання сумнівного хостинг-провайдера.	Зловмисник отримав доступ до незашифрованої резервної копії ключів гаманця.

Можемо зробити висновки, що найбільшою загрозою є зберігання у незашифрованому вигляді важливих даних, використання сумнівних хост-провайдерів та використання занадто простої автентифікації користувача. У зв’язку з цим, існує необхідність у створенні криптогаманця, який забезпечить користувача впевненістю, що його приватний ключ не буде втрачено, або принаймні, розшифровано.

Розроблено криптогаманець, який відповідає всім вимогам: шифрування приватного ключа та зберігання його на носії при реєстрації користувача; хешування приватних даних користувача при реєстрації та зберіганні до бази даних; подвійна автентифікація та автентифікація за номером телефону користувача; зручність здійснення транзакції; підпис транзакції вибраним файлом з приватним ключем користувача після його дешифрування.

Інтерактивна взаємодія програмного застосунку криптогаманця з користувачем здійснюється через вікно головного меню. Складова криптогаманця включає в себе базу даних, шифрування та хешування даних, зберігання документів на приватному носії користувача (Рис.1).

Базові процедури, що забезпечують роботу криптогаманця: вхід або реєстрація; зберігання приватного ключа на носії; оновлення балансу; створення транзакції; витягування та дешифрування приватного ключа; підпис транзакції; отримання хешу транзакції.

Експериментальне дослідження розробленого криптогаманця підтвердило адекватність його функціонування відповідно до встановлених вимог. За результатами роботи розроблено самостійний програмний засіб зберігання та відправки активів для монети Algorand, що за рахунок подвійної автентифікації, шифрування приватного ключа, хешування приватних

даних користувача, а саме хешування номеру телефону, логіну та паролю, електронної адреси, забезпечило надійний захист у зберіганні криптоактивів та у створенні транзакцій. Даний додаток може оновлюватись та розширюватись. В майбутньому планується додати підтримку інших криптомонет.

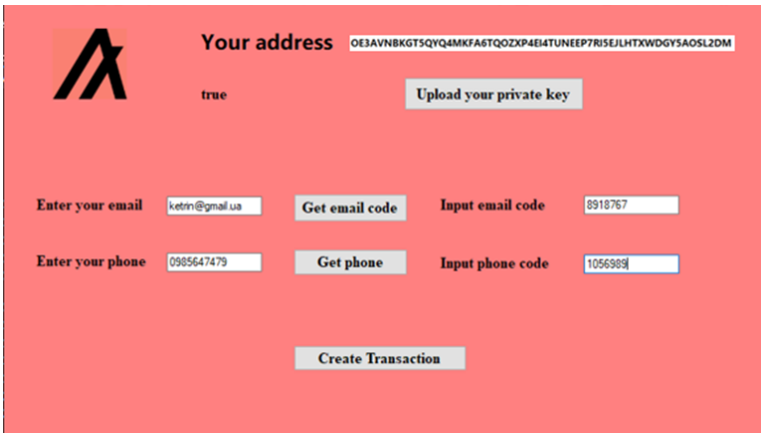


Рис.1. Вікно розробленого криптогаманця

СПИСОК ЛІТЕРАТУРИ

1. Regulation of Cryptocurrency Around the World" (PDF). Library of Congress. The Law Library of Congress, Global Legal Research Center. June 2018. pp. 4–5.
2. Golumbia, David (2015). Lovink, Geert (ed.). Bitcoin as Politics: Distributed Right-Wing Extremism. Institute of Network Cultures, Amsterdam. pp. 117–131.
3. Stallings, William (3 May 1990). Cryptography and Network Security: Principles and Practice. Prentice Hall. p. 165. ISBN 9780138690175.

ПРАВОВА ПОЗИЦІЯ ЩОДО ЗДІЙСНЕНИХ ЗЛОЧИНІВ З ВИКОРИСТАННЯМ HID-ПРИСТРОЇВ

Хлапонін Д.Ю., Драгунов П.І.
Київський національний університет будівництва і архітектури

Із стрімким розвитком комп'ютерних технологій вдосконалюються способи здійснення атак з боку зловмисників. Можливість використання різновидів типів атак створює відмінні умови для проведення тієї чи іншої атаки. З точки зору правової сили актуальним є Закон України [1], хоча в порівнянні з розвитком можливостей і бази знань зловмисників боротьба з останніми не є ефективною.

Згідно Кримінального кодексу України класифікація злочинів в сфері кібербезпеки базується в основному на статтях 361-363 Кримінального кодексу України. Через нездатність під час судового процесу об'єктивно розглядати й оцінювати позицію скоєних злочинів в сфері кібербезпеки існує глобальна проблема професійного аналізу та експертизи злочину. Одночасно Департамент кіберполіції України в силу свого вузького технічного напряму не зовсім коректно має можливість об'єктивно оцінювати злочини з юридичної точки з наступним рішенням в судовому процесі [2].

У даній статті ми будем аналізувати роботу HID-пристроїв. HID-пристрої - клас пристроїв USB для взаємодії з користувачем. Як HID можуть виступати такі периферійні пристрої як клавіатура, комп'ютерна миша, принтери і т.п. Для ефективного результату і для отримання інформації несанкціонованим доступом зловмисник використовує HID-пристрій як емуляцію натискань клавіатури. Іншими словами, за допомогою цього пристрою при підключенні до персонального комп'ютера на будь-якій операційній системі (Windows, Linux,

MacOS) відбувається з боку персонального комп'ютера ідентифікація пристроїв як клас пристрою взаємодії з користувачем, а саме клавіатури. Найчастіше отримання доступу до персонального комп'ютера шляхом незаконного доступу класифікується 361 статтею Кримінального кодексу України (несанкціоноване втручання в роботу електронно-обчислювальних машин, комп'ютерів, автоматизованих системах, комп'ютерних мереж або мереж електрозв'язку). При грамотній настройці HID-пристроїв зловмисник може отримати доступ не тільки до персональних даних, а й мати повне віддалене управління персонального комп'ютера. Досить підключити пристрій до персонального комп'ютера всього на 5-10 секунд, як вже відразу після підключення написаний сценарій, який завантажений в пристрій буде виконаний [3].

Складність захисту від подібних пристроїв полягає в тому, що більшість антивірусів, фаєрволів та інших ступенів захисту цей пристрій здатний обійти. Але не все так безнадійно. Для максимального захисту і забезпечення цілісності ваших файлів необхідно постійно оновлювати бази сигнатур, стежити за запущеними процесами, користуватися інтернетом з обережністю і відвідувати тільки довірені сайти. Також не рекомендується запускати виконувані файли такі як .exe, .tar.xz, exe.rar і т.п. При певних навичках зловмисник також може ховати виконувані файли під виглядом текстового документу або звичайною картинки (так звана «склейка»). В силу не ефективної роботи антивірусних програм і халатності користувачів, які забувають оновлювати бази сигнатур зловмисник має можливість завантажувати шкідливі файли без інформування користувача. Варто звернути увагу на програмне або апаратне закриття USB інтерфейсів з метою запобігання несанкціонованого підключення до персонального комп'ютера HID-пристроїв.

За розміром такі HID-пристрої зовні можуть виглядати як звичайний накопичувач і не представляти собою ніякої загрози до їх підключення до персонального комп'ютера. Сценарії коду можуть бути довільними, сам код в засвоєнні дуже простий, досить пару днів вивчення, щоб написати свій власний сценарій. Найпопулярніші HID-пристрої емуляції клавіатури є Rubbery Duck і Arduino Leonardo. Різниця між ними в основному полягає в ціні і складності налаштування. Для прикладу, перший пристрій коштує в середньому 50 $, коли другий в 10-13 разів дешевше. Але при цьому складність налаштування другого в рази більше. Сьогодні на просторах інтернету можна знайти багато модифікацій HID-пристроїв. З підтримкою технології Wireless, апаратно-інтегровані, модульні, багатофункціональні, з підтримкою кейлоггера і ін.

У даній статті для повного розуміння алгоритму роботи розглянемо HID-пристрій Arduino Leonardo. Для початку необхідно придбати HID-пристрій Arduino Leonardo Pro Micro на основі чіпа AtMega32U4. Після підключення до персонального комп'ютера немає необхідності встановлювати додаткові драйвери, за винятком офіційного програмного забезпечення Arduino. Після встановлення ПЗ вибираємо порт підключення пристрою і назву плати. Для коректної роботи будь-якого сценарію існують бібліотеки. У нашому випадку необхідно підключити бібліотеку «Keyboard.h». Без цієї бібліотеки коректна робота HID-пристрою не є можлива. При відсутності бібліотеки на локальному диску необхідно завантажити дану бібліотеку з мережі інтернет.

У відкритому доступі існує дуже багато сценаріїв виконання, але особливо варто приділити уваги класифікацій різних сценаріїв. Для Rubbery Duck існують одні сценарії, які не підходять для Arduino Leonardo. При завантаженні сценарію для іншого HID-пристрої в результаті сценарій не буде виконаний. Всі можливі сценарії є на відкритому майданчику Github з безкоштовною можливістю скачування. Також варто звернути увагу на глобальну проблему розкладки для подібних пристроїв. Всі команди написані виключно англійською мовою що робить запуск неможливим на іншій розкладці. Наприклад, якщо у користувача активна російська розкладка при підключенні HID-пристрої все команди будуть виконані російською мовою, що призведе до глобальної помилку виконання сценарію. З огляду на вищезазначене, підготовлені зловмисники знайшли рішення даної проблеми. Все полягає в

тому, що є можливість конвертувати символи в Alt-код. Таким чином, під час виконання сценарію емулюються клавіші за допомогою виконання Alt-коду відповідно до таблиці ASCII.

Таким чином, можна зробити висновок, що подібним атакам дуже складно протидіяти і навіть при наявності Firewall, антивіруса, інших компонентів безпеки не має гарантії повного захисту від подібних видів атак. Для забезпечення максимально можливого захисту необхідно фільтрувати накопичувачі, що підключаються, оновлювати бази сигнатур, робити аналіз запущених процесів на персональному комп'ютері, фільтрувати запуск виконуваних файлів і налаштовувати права доступу за різними категоріями. Потенційним зловмисникам нагадуємо статі 361 КК України, а саме: Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років.

СПИСОК ЛІТЕРАТУРИ

1. Закон України від 05.10.2017 № 2468-VIII «Про основні засади забезпечення кібербезпеки України».

2. Ємельянов, М. В. (2011). Поняття та види шахрайства за Кримінальним кодексом України. *Право і суспільство*.

3. Swarnalatha, G. (2021). Detect and Classify the Unpredictable Cyber-Attacks by using DNN Model. *Turkish Journal of Computer and Mathematics Education (TURCOMAT).*

ДЕТЕРМІНОВАНІ ЕФЕКТИВНІ АЛГОРИТМИ ВКЛАДЕННЯ БІТОВОГО ВЕКТОРА У ТОЧКУ ЕЛІПТИЧНОЇ КРИВОЇ, ЗАДАНОЇ У РІЗНИХ ФОРМАХ

Ковальчук Л.В., Кучинська Н.В., Теліженко О.Б., Панасюк І.І.
НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»

На поточний момент питання розробки детермінованих поліноміальних алгоритмів кодування бітових векторів в точки еліптичної кривої, яка може мати представлення у різних формах, є надзвичайно актуальним. Декілька напрямків робіт з теорії чисел та криптографії розглядали задачу детермінованого відображення у точки еліптичної кривої для використання у криптографічних протоколах, в основі яких лежить хешування або задача інкапсуляції ключа. Також процедура вкладення бітового вектора у точку кривої є необхідною для того, щоб мати змогу використовувати алгоритм шифрування Ель-Гамаля та алгоритми BLS-підпису. Варто зауважити, що до 2016 року існували лише ймовірнісні алгоритми вкладання вектора у точку кривої. Вони є набагато складнішими за детерміновані, а також взагалі не підходять для використання у алгоритмі шифрування Ель-Гамаля та алгоритмах BLS-підпису. Зазначимо, що вкладання випадкового бітового вектора з подальшим його однозначним відновленням для відповідного розшифрування є ще набагато складнішою процедурою, ніж вкладання значення геш-функції для побудови підпису.

Для детального розуміння цього питання необхідно розглянути основні відомості про еліптичні криві та їх форми. Після чого детально розглянемо проблему кодування елементів поля, над яким визначена крива, у множину точок.

Нехай $E = E\left(F_p\right)$ – еліптична крива у формі Вейерштраса над скінченним полем F_p що задається рівнянням:

$$E\left(F_p\right): y^2 = g\left(x\right), \quad де \;\; g\left(x\right) = x^3 + ax + b, \;\; a,b \in F_p, \;\; ab \neq 0\,. \qquad (1)$$

Припустимо, що бітовий вектор $k \in F_p$ (наприклад, якщо $p \geq 2^n$, то можемо розглядати вектор k як двійкове представлення деякого елементу $k \in F_p$, де n є довжиною вектора k).

Нашою метою є побудова детермінованого алгоритму, який виконує відображення $F_p \longrightarrow E\left(F_p\right)$ довільного елементу $k \in F_p$ в точку $Q_k \in E\left(F_p\right)$.

Така задача була вирішена у [1] для кривої у формі Вейерштраса. Також у бібліотеці [2] реалізовано відповідні алгоритми для всіх типів кривих у формі Вейєрштраса, включаючи криві, що задаються неповними рівняннями.

Проте крім форми Вейерштраса для застосування в криптографічних протоколах існують й інші форми представлення еліптичної кривої. Така різноманітність пояснюється тим, що кожна з таких форм має свої особливості та переваги, які й обґрунтовують їх використання.

Наприклад, рівняння еліптичної кривої в формі Монгомері має наступний вигляд:

$$M\left(F_p\right): By^2 = g\left(x\right), \quad \text{де } g\left(x\right) = x^3 + Ax^2 + Bx, \ A, B \in F_p, \ \left(A^2 - 4\right)B \neq 0, \tag{2}$$

Проте, якщо B є квадратичним нелишком за модулем p, то зручно використовувати еліптичну криву у формі Монтгомері в вигляді:

$$M\left(F_p\right): y^2 = g\left(x\right), \quad \text{де } g\left(x\right) = x^3 + Ax^2 + Gx, \ A, G \in F_p, \ \left(A^2 - 4\right)G \neq 0. \tag{3}$$

Зауважимо, що завжди можна перетворити криву в формі Монтгомері в криву в формі Веєрштрасса, але не навпаки.

Відносно недавно множина форм еліптичних кривих поповнилася новою формою, презентованою Едвардсом. Після цього оригінальна крива, запропонована Едвардсом, була з часом досліджена та модифікована іншими відомими вченими з метою покращення швидкодії операції додавання точок:

$$E\left(F_p\right): x^2 + ay^2 = 1 + dx^2y^2, \ a, d \in F_p, \ ad \neq 0, \ a \neq d, \ p > 2. \tag{4}$$

Важливою властивістю, що обмежує кількість кривих Вейерштраса, які можна представити в формі Едвардса, є те, що кількість точок еліптичної кривої у формі Едвардса завжди ділиться на 4. Основною причиною інтересу до еліптичних кривих у формі Едвардса є швидка арифметика додавання та подвоєння точок кривої, яка забезпечує суттєвий виграш у порівнянні з аналогічними операціями для точок еліптичної кривої у формі Вейерштрасса та Монтгомері. Таким чином, якщо криві, які вже використовуються в криптографічних протоколах, однозначно приводяться до форми Едвардса раціональними перетвореннями, тоді можна із використанням ефективних операцій швидкого додавання та подвоєння значно пришвидшити роботу таких протоколів.

Якщо для вкладення бітового вектора у точку еліптичної кривої, заданої у формі Едвардса або Монтгомері, використовувати її ізоморфізм кривій у формі Вейєрштраса, то алгоритм вийде занадто складним та переобтяженим, що зведе нанівець весь виграш у швидкодії. Тому необхідно розробити алгоритми вкладення бітового вектора у точку кривої у формі Монтгомері та Едвардса, які будуть вкладати відповідний вектор "безпосередньо" у криву відповідної форми, не використовуючи перехід до кривої у формі Вейєрштраса та потім зворотний перехід.

Основними результатами цієї доповіді є розробка, обґрунтування та побудова оцінок ефективності (за швидкодією та обсягом пам'яті) нових алгоритмів вкладання довільного бітового вектора у еліптичну криву у формі Монтгомері (для обох випадків) та у еліптичну криву у формі Едвардса. Ці алгоритми є простими та достатньо швидкими, їх безсумнівною

перевагою є те, що вони не потребують переходу до кривої у формі Вейєрштраса. При цьому алгоритм вкладання вектора у точку кривої у формі Монтгомері виявився навіть швидшим та зручнішим, ніж для кривої Вейєрштраса.

Алгоритм вкладання бітового вектора у еліптичну криву у формі Едвардса все ж таки використовує перехід до кривої у формі Монтгомері. Проте саме в цьому випадку перехід не сильно ускладнює створений алгоритм. В залежності від того, чи ділиться кількість точок кривої Едвардса на 8, при переході до кривої Монтгомері буде використовуватись рівняння кривої (2) або (3).

Також, крім зазначених алгоритмів, будуть наведені нові алгоритми вкладання бітового вектора у точку кривої, яка задається неповним рівнянням Вейєрштраса. До найбільш вживаних кривих з таким неповним рівнянням є крива, яка використовується для цифрового підпису у мережі Bitcoin [3].

СПИСОК ЛІТЕРАТУРИ

1. Wahby, Riad S. and Dan Boneh. “Fast and simple constant-time hashing to the BLS12-381 elliptic curve.” IACR Cryptology ePrint Archive 2019 (2019): 403.

2. Hashing to Elliptic Curves, https://tools.ietf.org/id/draft-irtf-cfrg-hash-to-curve-06.html

3. Математические основы биткойн-блокчейна. https://habr.com/ru/company/bitfury/blog/340378/

АТАКИ НА КВАНТОВІ КРИПТОГРАФІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Фесенко А.О.[1], Бердібаєв Р.Ш.[2]
[1]Національний авіаційний університет
[2]Алматинський університет енергетики та зв'язку імені Гумарбека Даукеева

Системи квантової криптографії до недавнього часу вважалися невразливими, так як в них, для забезпечення секретності інформації, використовуються не традиційні математичні методи, а робиться ставка на передачу інформації за допомогою об'єктів квантової механіки. Насправді квантові лінії зв'язку можуть захистити, наприклад, від атак типу «людина посередині». Однак, незважаючи на достатню надійність самої квантової лінії зв'язку, напрямком успішної атаки зловмисників може виявитися програмне забезпечення, яке здійснює передачу інформації, або інші уразливості конкретних програмно-апаратних реалізацій систем квантового розбраті поділу ключів[1].

Протягом останніх двох десятиліть небезпечними стають багато традиційних алгоритми криптографії: розподіл ключів, асиметричне шифрування і електронні підписи.

Одна з необхідних умов використання інформаційних технологій - забезпечення інформаційної безпеки: стану конфіденційності, цілісності і доступності даних. Більшість існуючих методів для вирішення цього завдання засновані на методах криптографії з відкритим ключем. В свою чергу це означає, що для захисту даних шляхом шифрування необхідно використовувати достатньо прості математичні операції, а для криптоаналізу потрібні колосальні обчислювальні ресурси.

Поява нового покоління обчислювальних пристроїв - квантових комп'ютерів - ставить під сумнів можливість використання сучасних криптографічних алгоритмів.

Зловмисник може вже сьогодні зберігати зашифровані традиційними методами дані, а з появою у нього доступу до квантовому комп'ютера розшифрувати їх.

Зокрема, за допомогою квантового алгоритму Шора стає можливим ефективним вирішення задач факторизації та дискретного логарифмування. Складність цих завдань забезпечує стійкість таких криптографічних примітивів, як RSA та ECDSA, що лежать в основі

більшості криптографічних засобів захисту інформації. Крім того, за допомогою квантового алгоритму Гровера можливий пошук за неупорядкованою базою даних з квадратичним прискоренням в порівнянні з найкращим класичним алгоритмом, що призводить до необхідності перегляду вимог щодо безпеки симетричних криптографічних алгоритмів. Завдяки постійному прогресу в квантових обчисленнях, вимоги до квантового комп'ютера, який здатний реалізувати алгоритм Шора постійно зменшуються.

Необхідність переходу на квантово-безпечні рішення активно обговорюється як науковим та діловим співтовариством, так і на рівні міжнародних регуляторів у сфері інформаційної безпеки.

Можливості квантової криптографії дозволяють в більшості випадків без проблем виявляти перехоплюючу сторону, але тим не менше при сучасних темпах прогресу з кожним роком для цього потрібно більше зусиль. Серед представлених атак, найбільший інтерес представляє атака з «осліпленням» лавинних фотодетекторів. Тут перехоплююча сторона залишається абсолютно непоміченою, що обумовлено визначальним недоліком квантової криптографії - низькою точністю ідентифікації передавальної і приймаючої сторін. Вирішити дану проблему можна за допомогою біометрії, шляхом створення автоматів, здатних дізнаватися просторово-віддалених користувачів квантового каналу і автоматично на малому прикладів їх біометричних образів

Одними з нових видів атак на квантові криптосистеми є атаки типу «Троянський кінь» та атаки, метою яких є віддалене управління детекторами легітимного користувача, яке здійснює несанкціонований користувач. Ці атаки можна віднести до класу «зумовлені недосконалістю обладнання».

Поряд з атакою «Троянський кінь» іншої значущої загрозою системам квантового розподілу ключів, в тому числі тим, що випускаються промислово, є виділені в окремий клас атаки, що отримали назву «віддалене управління детекторами одиночних фотонів з використанням адаптованого яскравого освітлення».

Аналогічний підхід був запропонований для атаки на системи квантового розподілу ключів. У літературі він отримав назву «атаки з використанням фальшивих станів». Спочатку атака на квантову криптосистему з використанням фальшивих станів позиціонувалася як різновид атаки «людина посередині», в ході якої Єва не намагається відновити вихідні стани, але генерує натомість світлові імпульси, які одержуються легітимними сторонами, не підвищуючи в комунікаційному каналі рівня помилок, що вказувало б легітимним сторонам на атаку. Відомо, що атака типу «людина посередині» на квантові протоколи розподілу ключів, яку називають ще непрозорою атакою або атакою «перехоплення – повторної посилки фотонів» ,приречена на невдачу, якщо Єва буде просто, без будь-яких додаткових заходів, направляти Бобу такі ж квантові стани, які виявлені нею при перехопленні та вимірюванні станів, відправлених Алісою.

Існує 2 можливих підходи для забезпечення захисту інформації при використанні квантових комп’ютерів для атак на сучасні криптографічні примітиви:

Квантові комунікації - припускає перехід на апаратні рішення, які використовують індивідуальні квантові стани світла (фотони) для передачі криптографічних ключів.

Постквантова криптографія - нові криптографічні алгоритми, стійкі до атак із застосуванням квантових комп'ютерів. Рішення на основі постквантової криптографії швидше інтегрувати, простіше оновлювати і вони дешевші.

Квантова криптографія повільно залишає суто академічне середовище і починає з'являтися в комерційних продуктах Теоретичні аспекти безпеки є дуже активною сферою досліджень, але порівняно небагато зроблено з точки зору вивчення практичних систем. Однак зростає інтерес до розгляду побічних каналів, що виникають внаслідок фізичної реалізації в практичних системах. Ми показали тут, як частина інформації, відкрито розкрита сторонами, що спілкуються, в зрілих реалізаціях, може призвести до того, що значна частина ключів стає небезпечними.

СПИСОК ЛІТЕРАТУРИ

1. Уязвимости реализации систем квантовой криптографии Vulnerabilities of quantum cryptography systems implementations : ст в жур. / науч. ст. Караммаев М.М., Топорков С.Е., Короченцев Д.А., Смирнов И.А., Черкесова Л.В. Ростов-на-Дону: Научное обозрение. Технические науки, 2020. ил., табл. – Текст: рос., англ. – Режим доступа: https://elibrary.ru/item.asp?id=43030019
2. Боне, Д. та ін. Випадкові оракули в квантовому світі. Досягнення криптології ASIACRYPT 2011. DH Lee and X. Wang, eds. Спрінгер.
3. Боне, Д. та Жандрі, М. Захист підписів та обраний захист зашифрованого тексту в світі квантових обчислень. *Досягнення криптології CRYPTO 2013.*Springer, 361379.
4. Gagliardoni, T., Hülsing, A. and Schaffner, C. Семантична безпека та невідмінність у квантовому світі. *Досягнення криптології* CRYPTO *2016.* M. Робшоу та Дж. Кац, ред. Спрінгер, 6089.

КРИТЕРІЇ ПОБУДОВИ СИСТЕМИ МОВНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ

Бєлозьорова Я.А., Зибін С.В.
Національний авіаційний університет

В даний час популярним являється підхід до ідентифікації особи, заснований на порівнянні спектральних характеристик мови цієї особи. Необхідно відзначити, що стандартна реалізація цього підходу призводить до низького ступеню ідентифікації особи. Однак, як показали виконані дослідження, використання окремих допоміжних алгоритмів дозволяє значно підвищити точність ідентифікації. З цією метою необхідно розглянути спільне використання алгоритмів ідентифікації на основі спектральних характеристик мови та ідентифікації на основі статистик основного тону. Перший підхід заснований на тому, що геометрія мовного тракту унікальна у кожної людини і цей факт знаходить відображення в різних спектральних характеристиках мови різних людей. Другий підхід з використанням основного тону, як компоненти мовного сигналу, крім інформації про поточний емоційний стан мовця, його інтонації, несе на собі індивідуальний, характерний для даної особи відбиток і вже досить тривалий час використовується для ідентифікації особи.

Найбільш явно відмінність спектральних характеристик проявляється в розташуванні формант в вокалізованих відрізках мовлення. Гельмгольц в своїх роботах чітко вказав особливості побудови моделі для ідентифікації мови і мовоутворення, в яких особливу увагу приділив наступним формантам:

- процес мовоутворення складається з двох незалежних компонент: порушення як такого звуку і формування фонетичного якості звуку за рахунок збудження резонансних частот артикуляції тракту (по Гельмгольцу) або фільтрації (в сучасному підході);
- фонетична якість елементарних мовних одиниць, визначається так званими формантами, які визначаються як резонансні частоти артикуляції тракту.

В такому випадку одним із найважливіших завдань стає точне автоматичне визначення положення формант. Однак, як виявилося, навіть досить грубо виділені формантні частоти є стійкими до шуму і характеристик каналу параметрами, що дозволяють здійснювати автоматичну ідентифікацію особи.

Для прийняття рішення здійснюється відстеження положення формант у вхідному сигналі і порівняння з шуканими особами в базі даних. Обчислення і порівняння формант здійснюється на коротких кадрах за обмеженою кількістю відліків, по формантного характеристикам яких обчислюється дистанція до осіб, представлених в базі осіб і вибираються найбільш близькі кандидати.

Підхід до ідентифікації на підставі спектральних характеристик можна розбити на кілька послідовних етапів:

1. Виявлення та видалення пауз, телефонних сигналів, характерних шумів не властивих мові особи.

2. Поділ на особи.

3. Шумоочистки і нормалізація.

4. Виділення ідентифікаційних характеристик кожної особи, формування бази еталонів.

5. Визначення приналежності однієї сукупності шляхом порівняння отриманих ідентифікаційних характеристик особи зі стандартним набором ідентифікаційних характеристик свідомо чужих осіб.

В якості ідентифікаційних ознак використовуються положення максимумів (3-х або 4-х), по можливості максимально відповідних формантам, на кожному спектральному зрізі, де їх вдалося досить надійно визначити. Дані ознаки в найбільшою мірою визначають індивідуальні особливості мовного тракту мовця.

Крім того, у зв'язку з особливостями мовного тракту його індивідуальність може характеризуватися такими параметрами, похідними від основного тону:

• середня частота і дисперсія основного тону;

• розподіл періодів основного тону;

• амплітудна модуляція основного тону;

• частотна модуляція періодів основного тону;

• співвідношення тривалостей дзвінких і шумових сегментів мовного повідомлення;

• контур основного тону на фразі;

• форму хвилі мовного джерела.

Представлені параметри добре описують індивідуальні характеристики мовця при відомих параметрах основного тону. Однак присутня складність застосування інформації про основний тоні в процесі розпізнавання особи, яка обумовлюється складністю поділу варіативності цього параметра в залежності від особи і в залежності від інших умов. З іншого боку, дослідження показують, що основний тон несе значну кількість інформації про особу. Як це показано в [2], знищення залишкової інформації про основний тоні в складі стандартних мел-кепстральних ознак тягне за собою 50% відносне погіршення продуктивності розпізнавання (з 10.7% до 16.7% EER). У статті [3] описується система, яка поєднує інформацію про частоту основного тону та хвильову структуру мови. Поєднання засноване на припущенні про умовну незалежності основного тону і хвильового пакета. Дане твердження спірне, але як показано в статті, додавання інформації про основний тон підвищує продуктивність розпізнавання мовця.

На підставі вищевикладеного можна виділити наступні основні етапи реалізації системи мовної ідентифікації особи.

Вимірювання фрактальної розмірності компонентів сигналу. Простий в реалізації етап, але досить ефективний в наборі всіх заходів розрізнення. Реалізація його можлива як з постійним вікном, так і з адаптивним типом вікна.

Визначення меж фрази. Для вирішення даного завдання найбільш раціонально використовувати запропоновані в роботах [1] алгоритми сегментації мови на основі мультифрактального підходу. На основі цього підходу в тих елементах сигналу, де зміна фрактальної розмірності перевищує деякий встановлений поріг, передбачається, починається фраза.

Виділення основного тону. Для вирішення завдання виділення основного тону існує необхідність розробки перешкодостійкого методу поперіодного виділення основного тону. В якості базового алгоритму виділення основного тону може бути взятий алгоритм [4,5], заснований на використанні апроксимації сигналу вейвлетом Морле з подальшим статистичним аналізом розподілу вейвлет-максимумів, що фізично пояснюється наявністю самоподібних структур характерних для сигналів, пов'язаних з резонатором.

На етапі вимірювання основного тону на ділянках сигналу має сенс порівнювати ні абсолютні величини, а нормовані – це дозволяє більш точно розрізняти особу по інтонаційному забарвленню.

Виділення характерних параметрів основного тону. Для вирішення цього завдання можна скористатися використанням тільки деяких з розглянутих параметрів при пофрагментному аналізі: середньою частотою і дисперсією основного тону; розподілом періодів основного тону; амплітудної модуляцією основного тону; частотною модуляцією періодів основного тону.

Порівняння параметрів сигналу з еталонними параметрами. Після здійснення процесу порівняння параметрів мови з еталонними потрібно вибрати з бази найбільш "близьку" особу. Для цього необхідно порівняти виділені параметри основного тону з бази на основі імовірнісного підходу.

В результаті проведеного дослідження встановлено структурні компоненти системи текстонезалежної мовної ідентифікації. Запропоновано використання конкретних алгоритмів знаходження основних параметрів цифрового мовного сигналу для реалізації в структурних компонентах системи, що розробляється. Як подальших досліджень показана необхідність розробки завадостійких методів поперіодного виділення частоти основного тону для реалізації систем текстонезалежної ідентифікації особи.

СПИСОК ЛІТЕРАТУРИ

1. Брюханова Я.А. Идентификация заданных фрагментов в звуковых файлах / Я.А.Брюханова, В.И. Соловьев // Вісник Східноукраїнського національного університету им.В.Даля. – Луганськ : Видавництво ВНУ ім. В. Даля , 2008. - № 9(127) ч.2. – С. 30-33.
2. Labutin Pavel V., Koval Serguei L. and Raev Andrey N., "Automatic Speaker Recognition Using Formants-Based Nearest-Neighbor maDistance Measure" // Proceedings from the 4th European Conference on Speech Communication and Technologies, "EUROSPEECH'95", vol.1, p.341.
3. Arcienega M., Alexander A., Zimmermann P., Drygajlo A. Bayesian Network Approach Combining Pitch and Spectral Envelope Features to Reduce Channel Mismatch in Speaker Verification and Forensic Speaker Recognition // Proceeding of Interspeech'2005, Lisbon, Portugal, Sept. 4-8, 2005. P. 2009-2012.
4. Рыбальский О.В., Соловьев В.И., Журавель В.В., Шабля А. Новий напрям рішення комплексу проблем фоноскопії // матеріали II-ої міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем". - 2013. - С.122-123.
5. Bielozorova Yana: Analyse and develop the software of automatic search for an anonymous person in the voice database // ITHEA International Journal "**Information Technologies & Knowledge**" Volume 13, Number 2 - 2019 – 152-164.

ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ У СИСТЕМАХ ОБРОБКИ ВЕЛИКИХ ДАНИХ

Дорожинський С.А.[1], Гнатюк С.О.[1], Охріменко Т.О.1, Юбузова Х.І.[2]
[1]Національний авіаційний університет
[2]Satbayev University, Алмати, Казахстан

Питання обробки великих даних все частіше з'являється в обговореннях найбільш відомих компаній світу, зокрема Microsoft, Amazon і Facebook, адже з кожним днем збільшується потік інформації, який потрібно постійно контролювати. У даній роботі представлено огляд найкращих напрямів розвитку сфери обробки великих даних та виявленні оптимальні варіанти для подальшої роботи.

Безліч особливостей всесвіту (починаючи від квантової заплутаність до деяких хімічних реакцій з великими молекулами) не можуть бути ефективно описані за допомогою звичайних комп'ютерів, заснованих на бінарній логіці. Рішення полягає в тому, щоб використовувати квантові процесори, які одночасно приймають декілька класичних станів, як це робить матерія. Однак для того, щоб такі квантові машини стали практичними, необхідно подолати безліч технічних перешкод. До них відносяться управління шумом і підвищення точності операцій, що впливають на квантові стани, які кодують інформацію.

Спільнота квантових обчислень направляє більшу частину своїх зусиль на створення досконалої машини: цифрового квантового комп'ютера, який витримує шум і помилки і який може бути застосований до будь-якої проблеми. Теоретично така машина, якій потрібні великі процесори, що складаються з безлічі квантових бітів або кубітів, повинна бути здатна робити обчислення швидше, ніж звичайний комп'ютер. До такої можливості принаймні 5-7 років. Для виправлення помилок потрібна надмірність, а кількість необхідних кубітів повинна швидко збільшуватись. Наприклад, для розкладання на множник 2000-бітне число за один день - завдання, яке неможливо вирішити на класичних комп'ютерах, буде потрібно 100 мільйонів кубітів, навіть якщо окремі квантові операції зазнають невдачі тільки один раз за кожні 10 000 операцій. Проте актуальною задачею на даний момент є зібрати цифрові квантові процесори з десятками кубітів. Такий консервативний погляд на квантові обчислення створює враження, що інвестори виграють тільки в довгостроковій перспективі. Проте короткострокова віддача можлива для невеликих пристроїв, які з'являться протягом наступних п'яти років, навіть якщо в них не буде виправлено всі помилки.

Відсутність теоретичних гарантій не має перешкоджати успіху. Евристичні «гібридні» методи, що поєднують квантовий і класичний підходи, можуть стати основою для потужних додатків майбутнього. Недавній успіх нейронних мереж в машинному навчанні - гарний тому приклад. У 1990-х роках, коли обчислювальні потужності, необхідні для навчання глибоких нейронних мереж, були недоступні, в цій області було модним зосередитися на «опуклих» методах (заснованих на функціях з чітким мінімальним рішенням), які мали сильну теоретичну основу. Сьогодні ці методи не підходять для глибокого навчання. Базові алгоритми нейронних мереж практично не змінилися, але завдяки закону Мура досягаються нові вражаючі рубежі продуктивності.

Масштаб, точність і керованість аналогового і цифрового квантового обладнання неухильно поліпшуються. Очікується, що через кілька років добре керовані квантові системи зможуть виконувати певні завдання набагато швидше, ніж звичайні комп'ютери, засновані на технології CMOS (додатковий метал-оксид-напівпровідник). Щоб отримати вигоду з неминучого прогресу в квантових технологіях, необхідно врахувати ряд вдосконалень. Апаратні поліпшення необхідні, щоб зробити пристрої досить надійними і керованими, щоб їх можна було використовувати для різних задач. Необхідно розробити евристичні квантові алгоритми, які вирішували б практичні проблеми в рамках поточних апаратних обмежень. Дослідники, що працюють над квантовими обчисленнями в Google, планують надати доступ до квантових процесорів через хмарні сервіси, щоб полегшити розробку і тестування квантових алгоритмів і програм в різних галузях, приносячи реальну користь суспільству.

Центральним і складним обчислювальним завданням у всіх кількісних дисциплінах фізичних і соціальних наук і в усіх галузях є оптимізація. Таку проблему важко вирішити за допомогою звичайних комп'ютерів, тому що алгоритми можуть дуже повільно переміщатися по математичному ландшафту можливих рішень; гарні рішення можуть бути приховані за високими перешкодами, які важко подолати. Найбільш загальні класичні алгоритми використовують статистичні методи (такі як розподіл теплової енергії), щоб подолати ці бар'єри. Цей тип класичної вибірки можна поліпшити, час від часу задіюючи квантові явища, такі як тунелювання (коли квантова інформація передається через бар'єри), щоб знайти рідкісні, але високоякісні рішення. Наприклад, в онлайн-рекомендаціях і стратегіях призначення ставок для реклами використовуються алгоритми оптимізації, щоб найбільш ефективно реагувати на потреби споживачів і мінливі ринки. Більш потужні протоколи,

засновані на комбінації квантових і класичних рішень, можуть поліпшити якість продуктів і послуг в багатьох галузях. Логістичним компаніям необхідно щодня оптимізувати планування і розподіл продукції. Квантово-доповнені алгоритми можуть поліпшити діагностику пацієнтів для охорони здоров'я, можна підвищити якість пошуку або рекомендацій по продуктах для великих компаній, що займаються інформаційними технологіями, такими як Microsoft, Amazon і Facebook.

Ще однією з провідних задач є квантова вибірка. Вибірка з імовірнісних розподілів широко використовується в статистиці і машинному навчанні. Теоретично ідеальні квантові схеми можуть здійснювати вибірку з більшого набору імовірнісних розподілів, ніж класичні схеми за той самий час. Розрахунки показують, що для відносно невеликих схем, що включають високоточні квантові ворота, можна буде зробити вибірку розподілів ймовірностей, які недоступні класично, використовуючи схему всього з 7 × 7 кубітів в шарах глибиною близько 25. Насправді, вибірка з розподілів з такою неглибокою квантовою схемою, ймовірно, стане першим прикладом "квантової переваги". Цей термін був придуманий фізиком-теоретиком Джоном Прескілом, щоб описати здатність квантового процесора виконувати за короткий час чітко певну математичну задачу, яку навіть найбільші класичні суперкомп'ютери (такі як китайський Sunway TaihuLight) не змогли б виконати протягом розумного періоду часу. Через кілька років буде проведено експеримент по досягненню квантової переваги. Серед перспективних застосувань квантової вибірки - висновок і розпізнавання образів у машинному навчанні. Щоб полегшити експерименти в академічних і промислових колах, також можна запропонувати доступ до квантового обладнання через інтерфейс хмарних обчислень.

Область квантових обчислень скоро досягне історичної віхи — квантової переваги. Досі невідомо, чи зможуть алгоритми, пов'язані з додатками, забезпечити значне збільшення швидкості з використанням тих типів процесорів, які незабаром будуть доступні. Але коли квантове обладнання стане досить потужним, з'явиться можливість перевірити це і розробити нові типи алгоритмів. Протягом наступного десятиліття наукові кола, промисловість і національні лабораторії повинні спільно розробити алгоритми квантового моделювання та квантового машинного навчання.

У даній роботі було розглянуто можливості впровадження квантових технологій до процесу обчислення великих даних, описано процеси оптимізації та квантової вибірки, а також перспективи в даній галузі. Було виявлено, що для у подальшому слід працювати над оптимізацією та квантовою вибіркою як над перспективними задачами в застосуванні квантових технологій для обробки великих даних.

СПИСОК ЛІТЕРАТУРИ

1. *Quantum Manifesto: A New Area of Technology* (Quantum Information Processing and Communication in Europe) [Електронний ресурс]. – 2016. – Режим доступу: http://go.nature.com/2im6rjr

2. Austin G. Surface codes: Towards practical large-scale quantum computation / G. Austin, M. Mariantoni. – 2012.

3. Boixo S. Computational multiqubit tunnelling in programmable quantum annealers / S. Boixo, V. Smelyanskiy, A. Shabani. – 2016.

4. Commercialize quantum technologies in five years [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.nature.com/articles/ncomms10327.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ

XIII Всеукраїнської науково-практичної конференції **SITS' 2021**

23-26 червня 2021 року
с. Коблево, Миколаївської області

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних уся відповідальність на авторів та їх наукових керівників.

Оригінал-макет підготовлено в
ГО «Асоціація спеціалістів кібербезпеки»