II Міжнародна науково-практична Інтернет-конференція

“Інновації та перспективні шляхи розвитку інформаційних технологій” (ІПШРІТ-2023)

м. Черкаси, 6 грудня 2023 року

Збірник тез доповідей

Міністерство освіти і науки України
Черкаський державний технологічний університет
Наукове товариство студентів, аспірантів, докторантів і молодих вчених ЧДТУ
Noosphere Engineering School
Техніко-гуманітарна академія (м. Бельсько-Бяла, Польща)
Університет Аделаїди (Аделаїда, Південна Австралія)
Національний університет харчових технологій
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»
Національний авіаційний університет
Національний технічний університет України «КПІ ім. Ігоря Сікорського»
Національний технічний університет «Харківський політехнічний інститут»
Центральноукраїнський національний технічний університет
Almaty University of Power Engineering and Telecommunications
(м. Алмати, Казахстан)

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІ Міжнародної науково-практичної інтернет-конференції

«ІННОВАЦІЇ ТА ПЕРСПЕКТИВНІ ШЛЯХИ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

(ІПШРІТ-2023)

6 грудня 2023 року

м.Черкаси

Черкаси
ЧДТУ
2023

УДК 004(063)

Затверджено рішенням вченої ради Черкаського державного технологічного університету, протокол № від 18.12.2023.

ПРОГРАМНИЙ КОМІТЕТ

Григор О. О. (д-р політ. наук, проф., в.о. ректора ЧДТУ) – голова оргкомітету

Заступники голови:

Фауре Е. В., д-р техн. наук, проф., проректор з науково-дослідної роботи та міжнародних зв'язків ЧДТУ;

Прокопенко Т. О., д-р техн. наук, зав. кафедри інформаційних технологій проектування.

Члени програмного комітету:

Mikolaj Karpiński, prof. (Poland, Bielsko-Biała); *Natali Lada*, PhD (Australia, Adelaide); *Rat Berdibaev*, PhD (Kazakhstan, Almaty); *Корченко О. Г.,* д.т.н., проф. (Україна, Київ); *Кучук Г. А*., д.т.н., проф. (Україна, Харків);*Смірнов О. А*., д.т.н., проф. (Україна, Кропивницький); *Єременко В. С*., д.т.н., проф. (Україна, Київ); Шостак І. В., д.т.н., проф. (Україна, Харків); Грибков С. В., д.т.н., доц. (Україна, Київ); *Рудницький В. М*., д.т.н., проф. (Україна, Черкаси); *Тесля Ю. М*., д.т.н., проф. (Україна, Черкаси); *Голуб С. В*., д.т.н., проф. (Україна, Черкаси).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Прокопенко Т. О., д.т.н., проф., зав. кафедри інформаційних технологій проектування – голова оргкомітету

Тарасенко Я. В., к.т.н., голова наукового товариства студентів, аспірантів, докторантів і молодих вчених ЧДТУ – заступник голови

Руденко В. О., аспірант (секретаріат)

Члени оргкомітету:

Тесля Ю. М., д.т.н., проф.; *Голуб С. В*., д.т.н., проф.; *Лавданська О. В*., к.т.н., доц.; *Рудницький С. В*., к.т.н., доц.; *Ланських Є. В.,* к.т.н., доц.

Контакти: бул. Шевченка 460, м. Черкаси, 18006.
Прокопенко Т. О. (097)2999979 t.prokopenko@chdtu.edu.ua
Тарасенко Я. В. (096)0377592 ya.tarasenko@chdtu.edu.ua

Збірник тез доповідей Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій» (6 груд. 2023 р., м. Черкаси) [Електронний ресурс] / упоряд. : Т. О. Прокопенко, Я. В. Тарасенко. М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2023. – 293 с.

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Інформаційний вибух – термін, що використовується вже понад п’ятдесят років та описує стрімке збільшення кількості об’єму даних і ефект, що виникає як наслідок. Зростання кількості доступних даних ускладнює процес управління інформацією. Зокрема, це стосується і конфіденційних даних, підтримка безпеки яких дуже важлива в теперішній час. Саме тому управління процесами запобігання витоку інформації є важливою та актуальною задачею.

Захист конфіденційної інформації є комплексним завданням оскільки існують різні канали її витоку. І одним з найбільш ефективним способом досягнення цього є впровадження технології запобігання витоку конфіденційної інформації Data Loss Prevention (DLP) [1]. Під DLP-системою зазвичай розуміють комплексне рішення, яке бореться з витоками інформації різними каналами. В рамках окремо узятого каналу DLP розглядається як «чорний ящик», де на вхід подається інформація, а на виході формується вердикт, чи належить вона до секретної. Отже основною цінністю такої системи є технології детектування, на основі яких працює «чорний ящик» [2]. Розглянемо основні із них. Сигнатури – найпростіший метод контролю, принцип полягає у пошуку певної послідовності символів у потоці даних. Цифрові відбитки – більш складний та ефективний підхід, передбачає створення різного типу геш-функцій зразків конфіденційних документів. Цифрові мітки – механізм призначення спеціальних міток всередині файлів. Регулярні вирази – метод знаходження збігів за регулярними виразами. Морфологічний аналіз – один з найпоширеніших способів виявлення витоків інформації, полягає в пошуку в тексті певних слів/словосполучень. Ручне детектування – перевірка інформації вручну. Кожен з розглянутих методів має свої переваги та недоліки, адже вимагає різного рівня модернізації системи та різного рівня зусиль на підтримку його ефективності.

Отже, проаналізувавши наявні методи детектування витоку інформації можна зробити висновок, що жоден з існуючих методів не може вважатися цілком надійним і ефективним, в різних випадках для забезпечення максимальної точності виявлення конфіденційної інформації потребується симбіоз декількох методів.

Список літератури

1. Чеботарьова Д.В., Пестєрєва С.Є. Аналіз технологій запобігання витоку інформації. «Проблеми інформатизації» : тези доповідей дев’ятої міжнародної науково-технічної конференції. Харків, 2021. С. 67.

2. Антонюк А.О., Портяной В.С., Шилін В.П. Технології захисту конфіденційної інформації від внутрішніх загроз. Проблеми програмування. 2011. № 1. С. 78-8

Пасічник Артем Олексійович

Викладач кафедри піротехнічної та спеціальної підготовки

Національний університет цивільного захисту України, м. Харків, Україна

ДИСТАНЦІЙНЕ НАВЧАННЯ, ЯК НЕДОСТАТНЬО РОЗВИНУТИЙ ЕЛЕМЕНТ БЕЗПЕКИ ОСВІТНЬОЇ ДІЯЛЬНОСТІ НА ТЕРИТОРІЇ УКРАЇНИ

Як визначає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»[1], інформаційна система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Саме ряд засобів ми й застосовуємо в усіх галузях нашого існування, і сьогодні є актуальним питанням у вирішенні щонайменше організації та проведення навчання. І з огляду на те, що цей закон начебто регулюю безпеку та захист інформації, чи дотримуємося ми його і як саме ворог користується цим? Як ми дійшли до цього та як саме необхідно сприяти національній безпеці?

Не зважаючи на те, що у 2013 році було розроблене положення про дистанційне навчання затверджене «Наказом МОН №466 від 25.04.2013 «Про затвердження Положення про дистанційне навчання»»[2], практичного застосування в Україні та актуальності воно не отримало, аж до поширення пандемії коронавірусу в 2020 році. Перш за все, не було в цьому потреби, оскільки освітяни, як наші, так і іноземці, мали змогу навчатися аудиторно. По-друге, ми не мали достатнього технологічного та технічного забезпечення. Цьому перешкоджали, як слабкий розвиток Інтернет покриття на території держави та матеріально-технічного забезпечення, так і фінансові можливості студентів, учнів чи слухачів, а також їх батьків. З поширенням інфекції довелося адаптуватися до онлайн навчання, або ж користуватися застарілими гаджетами, або ж купувати нові, також, доводилося придбати додаткові нові принади, такі, як наприклад, вебкамера чи гарнітура з мікрофоном, адже не в кожному будинку щоденно потрібні такі пристрої. Тож в період дворічного «домашнього» навчання, усі пристосувалися до такого режиму, хоча й рівень знань помітно знизився. Наступною причиною погіршення навчального процесу, його переналаштування стало повномасштабне вторгнення рашиської федерації. Найочевиднішим фактором зривання проведення занять стали постійні обстріли, тривоги та евакуації. Але завдяки нашим воїнам, Президенту та усім небайдужим людям на території України та усього світу, ми протягом цих двох років призвичаїлися до таких умов проведення. Звичайно ж, що нам доводиться, час від часу, сидіти без світла та Інтернету, але коли ці проблеми відходять на задній план, то як же ж ми організовуємо передачу інформації та здійснюємо освітній процес?

Не всі наші освітяни перебувають на території України, тож зателефонувати кожному немає змоги, маючи мобільний номер з нашим покриттям, яке не працює на території інших держав. Знову ж таки, маючи потік з, умовно кажучи, з 250-ма студентами, кожному телефонувати ірраціонально. Відповідно для зручності ми використовуємо месенджери. Найуживаніші з них, це Viber та Telegram, розробники яких є І.Магазинник та П.Дуров відповідно, отже, особи, які народилися на території країни агресори. Тому довіряти цим додаткам не варто, оскільки, не зважаючи на продаж цих програм, розробник може собі

залишити доступ до коду. Звичайно ж такі особи можуть бути завербованими ворожими спецслужбами. Підтвердженням цієї думки є опубліковані цитати з приватної розмови українського підприємця Ярослава Ажнюка з головою ГУР Кирилом Будановим. Чи можна довіряти WhatsAPP`у? З огляду на те, що розробники американці, то загалом можна, хоча й не всі громадяни цієї країни підтримують Україну у питанні збройного конфлікту та повернення територій, які визначені розділом другим статтею №3 Конституції України[3]. Також, варто пам'ятати про те, що в цьому додатку здійснюється збір інформації, і тому є потенційна загроза можливих хакерських атак з боку московітів. Непоганий за стосунок, яким користуються наші захисники, це Signal. Розробники якого є поляки, перші союзники, які допомогли нам, як зброєю, так і прилистком. І, перш за все, якщо ж ми свідомо обрали курс українізації, тоді варто спробувати та опанувати нашим вітчизняним зразком, а саме, Dober'ом[4], який у порівнянні з іншими месенджерами є найбезпечнішим та дійсно конфіденційним варіантом.

Наступним пунктом в організації та проведення занять є безпосередня зустріч зі студентами чи учнями у відеоконференціях. Найбільш розповсюдженою програмою для проведення онлайн занять є Zoom. Так, звичайно, він досить зручний та набув своєї популярності саме під час пандемії коронавірусу. Але, повертаючись до національної безпеки, безпеки інформаційних систем та українізації, варто наголосити на декількох проблемах, з якими стикаєшся, використовуючи продукт американської компанії. Рівень знань англійської мови серед українців усе ще недостатній, тому більшість з нас переводять мову сайту та самої програми на «собачу». Неодноразово спостерігав ситуацію з хакерськими атаками, пов'язаними з російсько-українською війною, а саме на інформаційному фронті. Жертвами ставали, як і свинорилі, так і наші співвітчизники, зокрема викладач НУЦЗУ. Тож, не зважаючи, на захищений доступ із використанням персональних ідентифікаторів та паролів, не зупиняє досвідчених хакерів. Варто спробувати та поширювати користування українського продукту, такого як Human[5]. Маючи захищені українські сервери, сервіс забезпечує безпеку проведення ваших занять з підтримкою рідної мови.

Отже, необхідно проводити повну українізацію освітнього процесу, а також закріпити на законодавчому рівні додатки, які сприяють захисту українських освітян. Забезпечити державну безпеку та розвиток вищевказаним застосункам.

Список літератури

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
2. Наказ Міністерства освіти і науки України від 25.04.2013 № 466 «Про затвердження Положення про дистанційне навчання»;
3. Конституція України;
4. Інтернет-посилання на офіційну сторінку Dober https://dober.chat/;