ТЕХНІЧНІ НАУКИ

Гальченко Я.О.
студент,
Київський політехнічний інститут
імені Ігоря Сікорського

ІНФОРМАЦІЙНА БЕЗПЕКА, ЯК СКЛАДОВА СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ФАКТОР ВПЛИВУ НА ТЕХНІЧНУ СФЕРУ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Сучасний етап загальносвітового розвитку інформатики характеризується зростаючою роллю інформаційної сфери. Перетворюючись на системотворчий чинник життя суспільства вона все більш активно впливає на стан політичної, економічної, оборонної, особистої, майнової і інших складових безпеки суспільства. Сучасні інформаційні технології істотно міняють не лише структуру стосунків, але і спосіб життя людей, їх мислення, механізми функціонування сім'ї, громадських інститутів, органів влади. Вони стають дієвим фактором розвитку особистості і суспільства. В той же час широке поширення деяких інформаційних технологій супроводжується появою ряду нових загроз конституційним правам і свободам громадян, формуванню здоров'я, повноцінного духовного життя. Ці технології вже використовуються для цілей економіки, торгівлі, реклами, політичної боротьби, чинячи іноді руйнівну дію на психіку людей, особливо підлітків. Інформаційний вплив стає головним важелем управління суспільством, все більше замінюючи фізичну дію, що тисячоліттями вважалася першочерговим засобом управління. Ось чому одним з основних елементів національної, громадської і особистої безпеки стає інформаційна безпека. У сучасному світі інформаційна безпека – життєва необхідна умова забезпечення інтересів людини, суспільства і держави.

В 1995 році в журналі «Нью-Йоркер» з’явилась всесвітньо відома карикатура про пса за комп’ютером, яка була підписана наступним чином: «В інтернеті ніхто не знає, що ти собака». Так от, минуло двадцять за гаком років, але в наш час все з точністю, але навпаки! Зараз, в сучасному інформаційному просторі кожна собака знає хто ти такий, а в деяких випадках навіть краще ніж ти сам. Про кожен клік, зроблений в браузері за замовчуванням повинні знати, як мінімум – дві сторони: клієнт і сервер. На даний проміжок часу можна визначити наступні ефективні способи захисту інформаційних ресурсів як для простого користувача так і для підприємства низької або середньої ланки:

- Використання програмного забезпечення, яке слідкує за станом програм та файлів, що ведуть статистику користування інформаційними ресурсами.

- Використання анонімного VPN (з безкоштовних HotSpot Shield).
- Уникнення програмного забезпечення, яке здатне записувати та вести історію використання інформаційних ресурсів та засобів передачі інформації.
- Користування лише достовірними інтернет-з'єднаннями.
- Використання антитрекінгових плагінів.
- Використання програм анонімного файл-шерінгу типу GNUnet, Freenet або I2P.
- Використання шифрування для захисту інформації.
- Слідкування за оновленнями вашого ПЗ.
- Використання антивірусних програмних засобів.
- Користування лише віртуальними банківськими картами.
- Використання лише протоколу HTTPS.
- Обов'язкова перевірка гіперпосилань.

Даний список звичайно не є вичерпним, але за спостереженнями автора являється найбільш оптимальним.

Слід зазначити, що приведені вище заходи являються не стільки макро скільки мікро-заходами, які стосуються кожного конкретного користувача, але також існують більш глобальні проблеми, вирішення яких потребує втручання світової спільноти. Важливим аспектом уникнення інформаційної небезпеки в автоматизованій системі є на думку автора використання на підприємствах, а особливо в державних установах і відомствах унікального програмного забезпечення, вихідний код якого є здобутком національних розробників програмного забезпечення, різноманітних національних дослідницьких центрів та інститутів. На практиці ж ми бачимо, що по суті практично одна-дві компанії, такі як Apple або Samsung, являються постачальниками практично усієї комп'ютерної техніки, засобів прийому, передачі та зберігання інформації призначених для державних потреб, які в свою чергу мають на увазі конфіденційність поширення інформації себе і своїх громадян. Слід зазначити, що дана тенденція прослідковується не лише з комп'ютерною та обчислювальною технікою, а й з різноманітними інтернет-сервісами (Google або Yandex), які реально являються монополістами у сфері інтернету і практично всі користувачі так чи інакше зберігають свої особисті дані та іншу цінну інформацію на серверах цих компаній, які до речі, є резидентами декількох певних країн, таких як США та Росія, а отже підпорядковуються їхньому законодавству, а значить і сфері зберігання, поширення та передачі інформації цих країн. Таким чином, цим країнам досить просто можна отримати будь-які дані про будь-якого громадянина в будь-якій точці планети про що свідчать не одноразові викривальні статті від WikiLeaks або минулих агентів спеціальних служб таких як Едвард Сноуден. Тому, як висновок, на світовому ринку має бути представлений увесь спектр різних компаній, а не тільки декількох монополістів, за якими стоять супердержави та капітали, котрі іноді більше за бюджети деяких країн третього світу.

Тому, на думку автора, вирішення проблеми забезпечення інформаційної безпеки як однієї конкретної особи так і цілої країни, повинно носити комплексний, системний характер і здійснюватись на різних рівнях, тому

можна виокремити декілька етапів: перший рівень – нормативно-документаційний; другий рівень – рівень інститутів; третій рівень – індивідуальний (особовий). На першому рівні органи державної влади повинні створити нормативно-документаційну базу, що враховує усі аспекти проблеми інформаційної безпеки. Другий рівень включає погоджену діяльність різних соціальних інститутів, пов'язаних з вихованням і соціалізацією, по забезпеченню інформаційної безпеки особи. Третій рівень пов'язаний, передусім, з самовихованням, самоосвітою, формуванням високого рівня інформаційної культури особи як частини загальної культури людини. На цьому рівні відбувається формування необхідних особових якостей для забезпечення інформаційного самозахисту особи.

Генча М.Е.
студент,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ВЕБ-СОКЕТИ – НОВИЙ РІВЕНЬ СПІЛКУВАННЯ БРАУЗЕРА І СЕРВЕРА

Вебсокети(WebSockets) це просунута і відносно нова технологія, що дозволяє відкрити постійне двонаправлене мережеве з'єднання між браузером користувача та сервером. За допомогою його API ви можете відправити повідомлення на сервер і отримати відповідь без виконання HTTP запиту, причому цей процес буде подієво-керованим.

В чому ж унікальність вебсокетів ? Для того, що відповісти на це питання розглянемо ситуацію:

Припустимо, що Ви вирішили написати додаток для розсилки. По-перше, треба зробити клієнт, який буде перевіряти, чи є нові повідомлення кожну хвилину. Проте, більшу частину часу не було ніяких нових повідомлень, а клієнт щохвилини посилатиме нові запити, викликаючи величезне навантаження на сервер. Цей метод був дуже популярний, і називався Polling. Ним і зараз користуються, навіть великі компанії (наприклад Вконтакті).

Якщо логічно подумати, то єдиним правильним рішенням буде зробити так, що сервер відсилав повідомлення на клієнт наскільки швидко, наскільки це можливо. Тобто клієнт не має ініціалізувати запит, цим має займатися сервер. Це було неможливо впродовж довгого часу, але як тільки була представлена технологія вебсокетів, це, нарешті, стало можливим.

Коли ви починаєте думати, єдиний висновок, що ви можете зробити те, що сервер повинен послати повідомлення клієнта, як тільки є пошта доступна. Клієнт не повинен ініціювати запит, а сервер повинен зробити це. Це було