На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.,** ректор ОНАХТ.

Співголови :
Капрельянц Л.В. – д.т.н., проф., проректор з наукової роботи та міжнародних зв′язків,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., доц., директор ННІМАтаКС ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри автоматизації виробничих процесів ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри технології і автоматизації виробництва радіоелектронних і електронно-обчислювальних засобів ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СПіСКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., директор інституту комп'ютерних технологій Національного авіаційного університету.

<u>Члени оргкомітету:</u>
Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ.
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ.
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ.
Грищенко І.В. – к.т.н., заступник декана ФІТта КБ ОНАХТ.
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

МЕТОДИ БЕЗПЕКИ ОСОБИСТОСТІ ПРИ ВИКОРИСТАННІ ІНТЕРНЕТУ

Ткачук В.О. студент ОКР „бакалавр" факультету ІТ та КБ ОНАХТ
Керівник – ст. викл. каф. КІ Бондаренко В.Г.

Сьогодні в Інтернеті можна знайти все. Відвідати Лувр, прогулятися вулицями Праги, подивитися заборонений фільм, прочитати скандальну книгу. Але все це дрібниці, порівняно з тим, що в інтернеті можна знайти особисту інформацію про будь-яку людину нашої планети. Ми йдемо до того, що особисте життя людини ставати громадської, а конфіденційність втрачається без нашої згоди. Відкриваючи за допомогою мишки і клавіатури двері в віртуальний світ, не забувайте, що ці двері може служити, не тільки для Вашого виходу, але і для входу до Вас. Легковажне користування Всесвітньою павутиною може привести до великих неприємностей, а то і трагедій в майбутньому. Вже сьогодні за кожним користувачем йде незримий і автоматизована стеження. В яких місцях буває, з ким розмовляє, що шукає в мережі інтернет. Сучасні операційні системи навчилися аналізувати практично всю інформацію про людину, а в найближчому майбутньому вони зможуть складати психологічний портрет, що дозволить обчислювальним машинам мати інформації про людину більше, ніж він сам знає про себе. У зв'язку з цим, кожному, хто не бажає, щоб його особисте життя стала надбанням інтернету, варто виконувати деякі правила.

Маскування в соціальних мережах. ВК, ФБ, ОК, Твіттер, інстаграм - все це повністю розкриває людини. Не треба бути досвідченим психологом, щоб по сторінці в соціальній мережі скласти портрет людини. Чим захоплюється, яких поглядів дотримується, з ким спілкується, що подобається. За музиці, яку слухає користувач, можна зрозуміти його схильності характеру, а іноді прорахувати його настрій в деякі дні. Всім цим користуються соціальні хакери, з метою отримати закриту інформацію. Звичайно, самий надійний спосіб замаскуватися - це не використовувати соцмережі. Але якщо Ви так вже товариські і не мислите себе без мережевого спілкування, то варто користуватися такими правилами:

1. Не намагайтеся докладно заповнювати свій профіль, а якщо заповнили, в налаштуваннях приватності сховайте доступ до нього для всіх. І уважно читайте угоду користувача, які гарантії конфіденційності надає Вам власник сайту.

2. Змініть своє прізвище на будь-яку іншу - це не дозволить Вас дуже легко знайти. Використовуйте третю прізвище в пошті gmail, ця маленька хитрість не дозволить зіставити інформацію про Вас з соцмережі з історією пошуку.

3. Не слід вказувати інформацію про Вашого особистого життя, не потрібно ставити статуси, не варто завантажувати фотографії з коханою людиною, на Вас можуть впливати через нього шляхом підтасовки фактів в інтернеті, або доведення до Вас обох неправдивої інформації один про одного.

4. Друзів, з якими ви дуже близькі, рекомендується приховати і зробити видними тільки Вам. Інакше зловмисник зможе впливати на вас через них, як і у випадку з Вашим улюбленим.

5. Для максимального захисту, намагайтеся видаляти діалоги, не зберігайте листування. Ще латиняни говорили: Verbavolant, scriptamanent (рус.аналог Слова летючий, письмена живучі).

Маскування при перегляді інтернет - сторінок. День у день кожен з нас робить близько 3-5 запитів в пошукових системах. Вся ця інформація зберігається і аналізується. На основі цього, мінімум що пропонується - реклама, відповідна Вам. Але крім цього, пошукові роботи знають про Ваші переваги, локаціях які відвідуєте, людей з якими спілкуєтеся. Високий рівень хакер, отримавши доступ до вашого облікового запису зможе все це відтворити. Для того, щоб себе убезпечити, варто виконувати наступні правила:

1. Встановіть в свій браузер плагін з сімейства «CleanHistory» (наприклад, Click & Clean або HistoryEraser або SingleClick) - він дозволить автоматично чистити кеш і видаляти історію з Вашого комп'ютера.

2. Видаліть всю історію пошуку, а також вимкніть її запис. Для цього перейдіть за посиланням history.google.com, зайдіть в розділ налаштування і переведіть повзунок в режим вимкнено. А також в налаштуваннях виберіть розділ «Видалення» і зітріть історію за весь період.

3. Підключіть плагін з сімейства Adblock, щоб відключити поява на екрані монітора настирливої і вірусної реклами.

4. У налаштуваннях свого мобільного телефону відключіть збереження історії розташування.

5. Уважно дивіться на посилання, які Вам надсилають. Можливо це фейк, з якого крадуть паролі. Наприклад, посилання vk.com- офіційний домен соціальної мережі «ВКонтакте», а посилання vk.3dn.ru - фейк, з якого крадуть паролі.

І, нарешті, правила банківської безпеки.

При оплаті банківською картою в інтернеті ніколи не погоджуйтеся на пропозицію зберегти дані карти в браузері. При оплаті в кафе або ресторані не давайте карту офіціантові в руки. Якщо він сфотографує карту з двох сторін, в подальшому доклавши певних зусиль, зможе перевести в готівку її.

Ніколи не зберігайте важливі документи в хмарі (дропбокс, гуглдіск, яндекс диск і ін.). Так, це зручно. Але сервера не належать вам. У будь-який момент ви можете втратити важливий договір.

Список літератури

1. Центр безпеки, як забезпечити безпеку своїх даних в соцмережі // офіційний сайт компанії Microsoft. - URL: http://www.microsoft.com/ru-ru/security/online-privacy/social-networking.aspx (дата звернення 20.03.16).
2. Майк Скиба. Безпека в соціальних мережах // Антивірус Norton. - URL: http: //ru.norton.com/social-networking-safety/article (дата звернення 20.03.16).