УДК 659.3+340.68 (045)

ВПЛИВ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ ТА ОСОБИСТОСТІ

ЖУК Сергій Володимирович,
студент четвертого курсу
кафедри Автоматики та управління у технічних системах
Факультету інформатики та обчислювальної техніки,
Національний технічний університет України «Київський політехнічний інститут»

Стаття присвячена проблемі систематизації типів загроз інформаційній безпеці у всесвітній та локальних комп'ютерних мережах, визначено прикладні методи захисту від них.

Ключові слова: *комп'ютерна мережа, соціальна мережа, збереження інформації, людський фактор, захист інформації, накопичувач даних, троянська програма, підготовка спеціалістів.*

В еру інформаційних технологій і всебічного розповсюдження комп'ютерної техніки людство стикнулось з принципово новими загрозами для інформаційної безпеки кожного індивіда та держави в цілому. В сучасних умовах для збору та аналізу приватної інформації про особу або державну інституцію не обов'язково встановлювати «зовнішнє спостереження» чи прослуховувати засоби зв'язку – достатньо лише зайти в глобальну мережу Інтернет і провести пошук у відкритих джерелах! А за деякої винахідливості – зловмисники можуть заволодіти накопичувачем даних, використання якого було завершено у зв'язку з оновленням апаратного забезпечення, але у якому не були відповідним чином знищено цілі томи конфіденційних матеріалів.

Зараз у всесвітній мережі легко знайти уривчасті або вузькоспрямовані публікації по визначеній темі, в той час як друковані видання загромаджені великою кількістю теоретичного матеріалу, що рідко є практичним для користувачів. В той самий час значна кількість осіб, що працюють з нерозголошуваною інформацією, в тому числі і державного значення, мають катастрофічно поверхневі знання з фундаментальних принципів захисту електронних типів даних.

Сьогодні принциповим завданням є донесення знань про базові принципи безпеки у комп'ютерних мережах до осіб, які мають безпосереднє відношення до інформаційної безпеки держави та стратегічних об'єктів, але не є спеціалістами у сфері IT. В цій статті ми систематизуємо деякі типи загроз інформаційній безпеці у всесвітній та локальних комп'ютерних мережах, визначимо прикладні методи захисту від них.

Розпочнемо наш огляд з соціальних мереж - загрозі інформаційній безпеці, яку можна вважати новою навіть за швидкоплинним часом оновлення комп'ютерних технологій. Яскравий приклад – «Вконтакте», система створена в Росії під керівництвом Павла Дурова, зараз нараховує близько 90 мільйонів користувачів з країн СНД. За правилами цієї соціальної мережі користувач реєструється, зазначаючи (не обов'язково, але так робить абсолютна більшість) свої особисті дані – місце навчання, роботи, відпочинку, формує коло друзів – які можуть переглядати інші користувачі. При активному користуванні соціальними мережами індивід часто створює образ «ідеального себе», проводить години робочого часу у мережі, а його коло спілкування може розширюватися блискавично та неконтрольовано. Цікавим є дослідження професора Пауля Кіршнера (Paul Kirschner), який довів факт зниження академічної успішності на 20% у студентів, котрі активно користуються соціальними мережами. Очевидно, що така ситуація може бути неприйнятною при роботі з конфіденційною інформацією, а також, створює загрозу для попадання індивіду під вплив іншої особи або спільноти.

Продовжуючи знайомство з загрозами інформаційній безпеці у комп'ютерних мережах, складно оминути увагою питання розповсюдження вірусів та «троянських програм». Хоча це питання є первісною задачею системних адміністраторів, ми не можемо не акцентувати увагу на неймовірну кількість зайвої та зараженої вірусами інформації на комп'ютерах багатьох співробітників державних установ. Прикро, що висококваліфіковані майстри своєї справи не розуміють всю важливість найпростішої процедури щоденного оновлення антивірусних баз та встановлення найновіших версій ліцензійного програмного забезпечення. До їх відома необхідно доводити, що вірус може назавжди знищити інформацію на їх персональному комп'ютері, а деяке «шкідливе» програмне забезпечення – просканувати комп'ютер, за лічені хвилини викрасти паролі та переслати у будь-яку частину світу найпотаємніші документи. У сфері захисту комп'ютерних мереж від такого типу загроз можна брати приклад з Німеччини, яка відмовилася від ненадійно захищених та дорогих продуктів корпорації Microsoft (Windows, Office та ін.), замінивши їх на модифіковані системи Linux, розроблені спеціаль-

но для держустанов ФРН.

Питання пріоритету державного інформаційного продукту чітко визначено у [5], нам залишається лише додати, що в Україні існують підприємства, здатні надати для держустанов та установ, що працюють із конфіденційними матеріалами, необхідне програмне забезпечення. Важливо зазначити, що процес розробки та алгоритми цих програм можуть бути проконтрольовані СБУ та профільними відомствами.

Розглянемо іншу загрозу інформаційній безпеці – підхід багатьох установ та приватних користувачів до збереження та передачі файлів у комп'ютерних мережах. Так, неприпустимим є факт винесення та перезапису на будь які носії конфіденційної інформації – хоча б як банально це не звучало. Наведемо лише один приклад: у 2008 році співробітник британської компанії-підрядника PA Consulting загубив флеш-карту з особистими даними десятків тисяч небезпечних злочинців. Продовжуючи тему даних, які необхідно передавати у комп'ютерних мережах – важко оминути увагою файлообмінні веб-сервіси накшталт Upload.com.ua та Rapidshare.com. Їх користувачі залишають файли у загальному сховищі, звідки потім їх «скачують» адресати. Багато хто забуває, що без спеціальних налаштувань та шифрування розміщені у таких сховищах файли можуть бути доступні для всіх користувачів, і їх легко знаходити через пошук на головній сторінці. При вирішенні завдань передачі даних між відомствами доцільно впроваджувати закриті приватні мережі. У продовження теми захисту електронних даних не можна оминути увагою і питання утилізації - скажемо дуже коротко про апаратне забезпечення: слід категорично заборонити припинення використання будь-яких накопичувачів без їх попередньої підготовки та ліквідації записаних на них даних.

Як заключний штрих інформаційної безпеки держави та особистості розглянемо людський фактор. Важко посперечатись із тим, що надсучасні програмні та апаратні засоби інформаційної безпеки не завжди можуть захистити від тривіальної людської неуважності та халатності. Ми вважаємо за необхідність інструктувати державних службовців всіх рангів та будь-кого іншого, хто має доступ до державних та корпоративних таємниць щодо наступних тез: 1) пароль від операційної системи або скриньки електронної пошти не може складатися з написаного англійськими літерами імені цуцика, а має являти собою незв'язну цифро-символьну комбінацію довжиною більше 12 символів; 2) будь-який пароль втрачає сенс, якщо написати його на папірці, що приклеєний до монітору; 3) не варто відкривати всі гіперпосилання, що надходять від незнайомих або знайомих людей, попередньо не переглянувши саму строку гіперпосилання – зловмисники часто використовують домени типу «odnoclassniki.ru», видаючи їх за «odnoklassniki.ru»; 4) не слід відповідати без попередньої перевірки на запити «адміністраторів» та «провайдерів», які ніби то загубили пароль або інші дані користувача системи чи мережі – таким методом найчастіше користуються зловмисники; 5) проблема національного масштабу – використання піратського програмного забезпечення, яке нерідко містить в собі замасковані віруси.

Стисло оглянувши найбільш розповсюджені типи загроз інформаційній безпеці у комп'ютерних мережах, ми бачимо визначаючу роль людини у захисті інформації. Саме від професійної підготовки співробітників відповідних департаментів і залежить інформаційна безпека корпоративного і державного сектору. Ми впевнені, що ця стаття відкрила для читачів двері у цікавий та динамічний світ захисту та нападу на персональні комп'ютери та комп'ютерні мережі, зробила його більш захищеним та готовим до протидії загрозам, які породжує глобалізація та всюдипроникна комп'ютерна техніка.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Джедаєв А. Я люблю компьютерную самооборону: учебн. пособ. / А. Джедаєв. – М.: Только для взрослых, 2002. – 432 с.
2. Інтернет-видання «Information Security», режим доступу: www.itsec.ru
3. Інтернет-видання «Intelligent Enterprise», режим доступу: www.iemag.ru
4. Інтернет-видання «Социальные сети и социальный маркетинг в интернете», режим доступу: www.sociofan.ru
5. Указ президента України № 514/2009 «Про Доктрину інформаційної безпеки України»

Жук С. В. Влияние компьютерных технологий на информационную безопасность государства и общества / Факультет информатики и вычислительной техники Национального технического университета Украины «Киевский политехнический институт».

Статья посвящена проблеме систематизации типов угроз информационной безопасности во всемирной и локальной компьютерных сетях, определены прикладные методы защиты информации. В частности, обосновывается значительность роли человеческого фактора на всех уровнях защиты корпоративной и государственной информации.

Ключевые слова: *компьютерная сеть, социальная сеть, сохранение информации, человеческий фактор, защита информации, накопитель данных, троянская программа, подготовка специалистов.*

Zhuk S. V. Impact of computer technologies on information security of the state and society / National Technical University of Ukraine «Kiev Polytechnic Institute».

The article is devoted to the problem of systematization types of threats of information security in the world and local computer networks, applied methods of protection of the information are defined. In particular, relevancy of a role of the human factor at all levels of protection of the corporate and state information is proved.

Key words: *computer network, social network, information safety, human factor, information security, storage device, trojan program, expert training.*