УДК 004.056:004.49

ВПЛИВ КОМП'ЮТЕРНИХ ПРОГРАМ НА ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ НА ПРОМИСЛОВИХ ОБ'ЄКТАХ

Є.О. Семенов
Кандидат технічних наук, доцент*
Контактний тел.: (057) 707-69-59, 098-617-33-14
E-mail: semyonov_zhenya@ukr.net

О.В. Толстоусова
Асистент*
Контактний тел.: (057) 707-69-59
E-mail: tolstousova73@mail.ru

В.В. Березуцький
Доктор технічних наук, професор, завідуючий кафедрою*
Контактний тел.: (057) 707-66-65
E-mail: qwer@kpi.kharkov.ua
*Кафедра охорони праці та навколишнього середовища
Національний технічний університет "Харківський політехнічний інститут"
вул. Фрунзе, 21, м. Харків, Україна, 61002

Стаття присвячена проблеми виникнення надзвичайних ситуацій техногенного характеру внаслідок збоїв керуючих комп'ютерів на промислових об'єктах, проникнення до керуючих комп'ютерів комп'ютерних вірусів чи троянських програм

Ключові слова: комп'ютерні програми, віруси, надзвичайна ситуація

Статья посвящена проблеме возникновения чрезвычайных ситуаций техногенного характера вследствие сбоев управляющих компьютеров на промышленных объектах, проникновения в управляющие компьютеры компьютерных вирусов или троянских программ

Ключевые слова: компьютерные программы, вирусы, чрезвычайная ситуация

The article devoted to the problem of technogenic emergencies due to failures control of computers in industrial objects, the penetration of to the controlling computer of computer viruses, worms or trojan system programs

Key words: computer programs, viruses, emergency situation

1. Введення

У сторіччя, коли інформаційні технології досягли величезного поширення серед економічних об'єктів по всьому світу, над безпекою людства нависла загроза техногенних катастроф які причинені саме інформаційними технологіями. З кожним днем у мережі інтернет з'являється все більше різновидів комп'ютерних вірусів, що загрожують тепер не тільки нормальній роботі персональних комп'ютерів звичайних користувачів, але й роботі керуючих комп'ютерів на великих підприємствах. Кібернетичні атаки можуть стати ідеальним знаряддям наступних війн – вони стрімкі, ефективні у своїй руйнівній силі і, як правило, анонімні. Тому країни активно домовляються про сумісні стратегії протистояння кібернетичним загрозам [1].

2. Постановка проблеми

До недавнього часу комп'ютерні програми взагалі ніхто не розглядав як ймовірне джерело техногенної небезпеки. І тому у доступних джерелах відсутня узагальнююча інформація про вплив програмного забезпечення на утворення техногенних ситуацій. Ціллю даної статті є проведення літературного огляду проблеми впливу інформаційних технологій на надзвичайні ситуації на промислових об'єктах.

3. Дані про сучасний стан проблеми

На початку 2009 року в новинах почала з'являтися інформація про створення і поширення хакерами нового вірусу під назвою "Stuxnet", що вражає системи

диспетчерського управління і збору даних (SCADA) виробництва компанії Siemens AG. SCADA широко використовується по всьому світу у системах управління різноманітними об'єктами – аеропортами, будівлями, кораблями, очисними спорудами, водо-, газо- і нафтопроводами, підприємствами.

Відомо, що вірус-троян Stuxnet поширюється за допомогою флеш накопичувачів, використовуючи "діри" в операційній системі Windows. На думку фахівців, вірус може використовуватись як за для промислового шпигунства, так і для саботажу. При роботи він встановлює зв'язок з іншим сервером, який може використовуватись для крадіжки даних або для отримання контролю над інженерними системами.

Проникнення вірусу спостерігалося по всьому світу. Наприкінці вересня стало відомо, що вірус Stuxnet завдав серйозної шкоди іранській ядерній програмі – зірвав терміни запуску ядерної АЕС в Бушері. Використовуючи вразливість операційної системи і "людський фактор", Stuxnet успішно вразив 1368 із 5000 центрифуг на заводі по збагаченню урану в Нантанзі. Вірус Stuxnet проникав до двох Німецьких АЕС [2, 3].

Наприкінці вересня 2010 року стало офіційно відомо, що вірус Stuxnet вразив багато промислових об'єктів Китаю. Всього було вражено близько 1000 великих промислових об'єктів, які китайські експерти так і не змогли захистити від проникнення вірусу, хоч інформація про розповсюдження цього вірусу давно була доступна [4].

На конференції Virus Bulletin 2010, що проходила у Ванкувері (Канада), увагу публіки залучила коротка доповідь Liam O'Murchu, одного з провідних експертів Symantec по IT–безпеці. Аналітик зробив експеримент, що роз'яснює небезпечність кібер-загрози краще сотні формальних звітів. Він встановив на сцені повітряний насос, що працює під керівництвом операційної системи виробництва Siemens, інфікував робочу станцію, що контролює насос, вірусом Stuxnet і запустив процес у дію. Насос швидко надув повітряну кулю, але процес не закінчився – куля надувалася доки не вибухнула [5].

Декілька раніше атомна електростанція в штаті Джорджия в екстреному режимі призупинила роботу на 48 годин після того, як на одному з її комп'ютерів було проведено оновлення операційної системи. Інцидент стався 7 березня 2008 року на атомній станції Хетч неподалік від міста Бакслі. Проблеми розпочались після того, як інженер з компанії, що займається технологічним обслуговуванням станції встановив оновлення на головний комп'ютер мережі АЕС. Комп'ютер використовувався для стеження за хімічними даними і діагностики однієї з основних систем електростанції. Згідно доповіді Nuclear Regulatory Commission, після встановлення оновлень комп'ютер планово перезавантажився, але при цьому були втрачені дані керуючих систем. Втрата даних була розцінена системою безпеки станції як викид радіоактивних речовин в системі охолодження реактору. В результаті, автоматична система безпеки зупинила усі процеси на станції [6].

Крім атомних електростанцій багато компаній, а особливо авіакомпаній, страждають від збоїв у роботі керуючих комп'ютерів. Через збої комп'ютерів, що контролюють усі внутрішні лінії, виникають багаточасові затримки і збої у розкладі залежних авіакомпаній.

20 листопада 2009 року, за даними федерального авіаційного управління США, збій в системі порушив повітряне сполучення між аеропортами всієї території країни. Авіакомпаніям довелось відмінити або відкласти сотні рейсів. За словами офіційного представника федерального авіаційного управління США Арлін Селак, проблема виникла близько п'ятої ранку у серверах управління, що розташовані у в Солт–Лейк–Сіті і Атланті. Подібний випадок стався в США в серпні 2008 року [7].

1 липня 2009 року зазнав аварії Аеробус А330 компанії Air France. Експерти вважають, що однією з причин аварії міг стати збій в комп'ютерній системі управління літаком. Сучасні пасажирські лайнери, до числа яких входить Аеробус А330, що вилетів з Ріо-де-Жанейро, оснащуються системою Air Data Reference Unit (ADRU). Ця система відповідає за передачу інформації, включаючи висоту польоту і швидкість вітру, на альтиметри в кабіні пілотів і інформаційні дисплеї. Ця ж система забезпечує даними автопілот. Приймаючи до уваги даний факт, легко уявити, що якщо ADRU раптом почне надсилати помилкову інформацію – це може призвести до катастрофи. ADRU вже декілька разів ставала причиною небезпечної поведінки повітряних судів. Повідомлялось, що система може завдати труднощів при отриманні критично важливих даних для здійснення безпечного польоту і завдати труднощів під час ручного управління літаком [8].

Є і інші дані про випадки на різних об'єктах. Так 11 листопада 2009 року в окрузі Монгомері (штат Меріленд в США) було зафіксовано вихід з ладу комп'ютерної системи, що скеровує роботу 750 світлофорів на території округу. Збій системи спричинив перевід всіх світлофорів в автономний режим роботи, що в свою чергу спричинило декілька аварій, виникнення на дорожніх магістралях багатокілометрових пробок [9].

В 2009 році були помічені випадки аварій при участі автомобілів Toyota, спричинених тим, що автомобілі збільшували швидкість, виходячи з-під контролю водіїв. За словами власників Camry, Prius і Lexus, потримані автомобілі раптом самостійно різко набирали швидкість приблизно 100 миль за годину, і це ставало причиною аварій. Усього було зафіксовано 2000 подібних випадків. Водії стверджували, що педалі під час інцидентів вижимались справно, і пов'язують те що трапилось зі збоями в комп'ютерній системі автомобіля [10].

Збій в комп'ютерній системі змусив японців готуватися до землетрусу. За заявою національного Метеорологічного правління країни, збій було спричинено «непотрібними удосконаленнями», що були внесені до системи компанією обслуговування [11]. Тривога в свою чергу призвела до значних перебоїв в роботі транспорту і створила чимало проблем для десятків тисяч пасажирів, що поспішали на роботу.

В квітні 2009 року комп'ютерна помилка стала причиною зникнення цілого озера в австралійському місті Аделаїда. Як стало відомо в результаті розслідування, через виникнення комп'ютерного збою автоматично були відкриті ворота греблі, що втримувала водний потік. Щезнення води в озері призвело до збитків річного пароплавства і круїзних кампаній [12].

3. Висновки

Таким чином проведений літературний огляд доступних даних показав, що сучасний розвиток науки і техніки привів до появи нової загрози для безпеки людини – це аварії і катастрофи які спричинені порушеннями у роботі комп'ютерних систем. Ці порушення можуть виникнути як через звичайну людську недбалість або непрофесійні дії, так і в результаті дії спеціально створених зловмисниками комп'ютерних програм – вірусів чи троянських програм.

Литература

1. Stuxnet: война 2.0 /http://habrahabr.ru/blogs/infosecurity/105964/.
2. Stuxnet таки добрался до иранского ядерного завода в Бушере /http://habrahabr.ru/blogs/infosecurity/104973/.
3. Вирус-троян пробрался в промышленные сооружения /http://www.bfm.ru/news/2010/07/20/virus-trojan-probralsja-v-promyshlennye-sooruzhenija.html.
4. Stuxnet поразил более 1000 предприятий Китая /http://habrahabr.ru/blogs/infosecurity/105316/.
5. Stuxnet. Истерия продолжается... /http://habrahabr.ru/company/eset/blog/105507/.
6. Атомная электростанция прекратила работу из-за обновления ПО
7. /http://www.securitylab.ru/news/354480.php?page=user&id=56946.
8. В США сотни рейсов отменены из-за компьютерного сбоя /http://www.securitylab.ru/news/387926.php.
9. Причиной крушения самолета Air France мог стать компьютерный сбой
10. /http://www.securitylab.ru/news/380975.php.
11. США: 750 светофоров отключились из-за сбоя компьютера /http://www.securitylab.ru/news/387612.php.
12. Автомобили Toyota попадают в аварии из-за компьютерного сбоя
13. /http://www.securitylab.ru/news/387414.php.
14. Из-за компьютерного сбоя японцы получили ложное предупреждение о землетрясении /http://www.securitylab.ru/news/384258.php?page=user&id=81026.
15. Компьютерный сбой уничтожил австралийское озеро
16. /http://www.securitylab.ru/news/378652.php.

УДК 519.72

ИНФОРМАЦИОННЫЕ АСПЕКТЫ ПРИ РАЗРАБОТКЕ СЕНСОРНЫХ СЕТЕЙ (ЧАСТЬ 2)

В.А. Иваненко
Аспирантка*
E-mail: zlata_ne@bk.ru

А.Н. Зеленин
Кандидат технических наук, профессор*
Контактный тел.: (057) 345-00-83
*Кафедра «Сети связи»
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, 61166

Використовуючи теоретико-інформаційну концепцію вибору за К. Шенноном у рамках інформаційних систем, – сформульовані умови забезпечення працездатності бездротових сенсорних мереж, що самоконфігуруються, за рахунок введення надмірності

Ключові слова: сенсор, мот, надмірність

Используя теоретико-информационную концепцию выбора по К. Шеннону в рамках информационных систем, сформулированы условия обеспечения работоспособности беспроводных самоконфигурируемых сенсорных сетей за счет введения избыточности

Ключевые слова: сенсор, мот, избыточность

In this article being formulated conditions to provide the efficiency of the wireless self-configurable sensor network using information-theoretic concept of selection of information systems by K. Shannon

Keywords: sensor, mote, redundancy

1. Введение

Стимулом к развитию прикладной теории информации явилась возможность решать такие задачи, которые, вследствие трудностей формализации или существенной неопределенности в формировании системной концепции (идеологии), не решались вообще или решались, но с меньшей полнотой, чем при ис-