МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»
ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА БЕЗПЕКИ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

РАДА МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

VII ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

26 березня 2015 р.

м. Дніпропетровськ

УДК [004+621.39](06)
І 74
ББК 32.973

Оргкомітет конференції:

Голова:	Декан факультету інформаційних технологій, д.т.н., професор Алексєєв М.О.
Заступник голови:	Голова ради молодих вчених факультету інформаційних технологій Мєшков В.І.
Члени оргкомітету:	д.т.н., професор Бабенко Т.В. д.т.н., професор Корнієнко В.І. д.т.н., професор Корсун В.І. к.ф.-м.н., доцент Гусєв О.Ю. к.ф.-м.н., доцент Магро В.І. к.т.н., доцент Удовик І.М. доцент Жукова О.А. ст. викл. Галушко С.О. ст. викл. Мартиненко А.А. ст. викл. Тимофєєв Д.С. ас. Гуліна І.Г. ас. Масальська О.О. ас. Мілінчук Ю.А. ас. Рибальченко Ю.П. ас. Торбєєва М.В.

І 74

Інформаційні технології. Безпека та зв’язок: Матеріали всеукр. наук.-практ. конф. – Д.: Державний ВНЗ «Національний гірничий університет», 2015.– 72 с.

Викладено тези доповідей учасників VII Всеукраїнської науково-практичної конференції «Інформаційні технології. Безпека та зв’язок», яка відбулася у Державному ВНЗ «Національний гірничий університет» 26 березня 2015 року. На конференції було розглянуті найбільш актуальні проблеми розвитку інформаційних технологій, безпеки та зв’язку в Україні та шляхи їх вирішення.

УДК [004+621.39](06)
ББК 32.973

ЗМІСТ

Секція «Інформаційна безпека»

ІСТОРІЯ РОЗВИТКУ КАФЕДРИ БІТ

Під кінець 50-х років XX ст. стали очевидними перспективність і важливість застосування досягнень електроніки та обчислювальної техніки в наукових дослідженнях, інженерних розрахунках, а також при вирішенні задач автоматизації управління виробництвом і технологічними процесами.

Враховуючи специфіку навчальних дисциплін з промислової електроніки та обчислювальної техніки, а також необхідність їх включення в робочі плани усіх спеціальностей, **2 вересня 1964** року на електротехнічному факультеті Дніпропетровського гірничого інституту була заснована спеціальна кафедра промислової електроніки та обчислювальної техніки.

Організувати кафедру та очолювати її доручили відомому вченому та педагогу, доктору технічних наук, професору **Володимиру Івановичу Жуковицькому**. На момент організації професорсько-викладацький склад кафедри налічував, окрім завідувача, 2 доценти та 5 асистентів. При кафедрі були обладнані перші навчальні лабораторії промислової електроніки (12 робочих місць) та обчислювальної техніки (7 робочих місць). До складу кафедри також увійшла науково-дослідна лабораторія електронно-обчислювальних машин та обчислювальної техніки.

З дня заснування і до сьогодення співробітники кафедри вели й ведуть дослідження за різними науковими напрямками. На ранньому періоді розвитку кафедри склалися два основних напрямки наукової роботи: «Розробка методів та систем автоматизованого проектування та управління гірничими підприємствами із застосуванням засобів обчислювальної техніки» та «Розробка технічних засобів для автоматизованих систем контролю та управління гірничими підприємствами».

Значних досягнень у науковій та педагогічній діяльності колектив кафедри здобув під керівництвом таких вчених, як професор **Бунько Віктор Олександрович**, доценти **Товстоног Микола Макарович** та **Трач Анатолій Іванович**, які очолювали кафедру в період з 1978 по 1993 роки.

З 1988 року кафедра носить нову назву електроніки та обчислювальної техніки (ЕОТ).

З 1993 по 2011 рр. кафедру очолював видатний вчений та педагог, доктор технічних наук, професор **Георгій Віталійович Кузнецов**. З 1993 року розпочався новий етап в історії кафедри.

На той час в університеті активізується робота по використанню комп'ютерної техніки і комп'ютерних технологій у навчальному процесі. На зміну застарілій техніці прийшли комп'ютери нового покоління – персональні ЕОМ.

У 1995 році керівництвом університету було прийняте рішення про перетворення кафедри ЕОТ зі спеціальної у випускаючу. У 1995 році відкрита спеціальність 7.080403 «Програмне забезпечення автоматизованих систем», а слідом за нею у 1996 році –

спеціальність 7.080401 «Інформаційні управляючі системи та технології». Спеціальності успішно пройшли акредитацію.

Зважаючи на авторитет вчених та науковців кафедри в галузі інформаційної безпеки з 1998 року кафедрі, одній з перших в Україні, надано право готувати спеціалістів за напрямом «Інформаційна безпека»:

у 1998 році відкрито спеціальність 7.160101 «Захист інформації з обмеженим доступом та автоматизація її обробки» ;

у 2001 році – спеціальність 7.160105 «Захист інформації в комп'ютерних системах і мережах» ;

у 2002 році – спеціальність 7.160104 «Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом» .

Враховуючи потреби регіону у фахівцях з телекомунікацій на кафедрі у 2003 році відкрито спеціальність 7.050903 «Телекомунікаційні системи та мережі» .

Завдяки авторитету вчених і фахівців кафедри, результативності їх науково-дослідної діяльності, в 1998 р. на базі Національної гірничої академії України створено Придніпровський регіональний науково-технічний центр технічного захисту інформації . До оснащення центра і роботи в ньому залучають також найбільш досвідчених фахівців з КБ «Південне», ПМЗ, ДМЗ та інших підприємств і організацій міста.

За час свого існування кафедра дала життя багатьом кафедрам і підрозділам університету. У 1970 році при кафедрі було організовано секцію математичних методів дослідження операцій. З вересня 1971 р. вона виділилася в окрему кафедру з такою ж назвою (нині кафедра системного аналізу та управління).

У 1970 році замість лабораторії електронно-обчислювальних машин та обчислювальної техніки при кафедрі було організовано відділ електронно-обчислювальної техніки, до складу якого увійшли держбюджетна група електронно-обчислювальних машин та обчислювальної техніки, а також штатний персонал НДС, що бере участь у виконанні науково-дослідних робіт.

У 1996 р. з колективу кафедри була виділена частина професорсько-викладацького складу для організації на економічному факультеті кафедри економічної кібернетики та інформаційних технологій.

У 2003 році з колективу кафедри виділена частина професорсько-викладацького складу для організації на факультеті інформаційних технологій кафедри програмного забезпечення комп'ютерних систем, що взяла на себе підготовку фахівців за напрямом «Комп'ютерні науки».

Професор Кузнецов Г.В. входив до складу експертної ради МОН України «Національна безпека» та до складу робочих груп з розробки державних стандартів у галузі «Комп'ютерні науки» та «Інформаційна безпека». У 1999 р. за значний особистий внесок у забезпеченні високого рівня підготовки фахівців, вагомі наукові досягнення доктору технічних наук, професору Кузнецову Г.В. було присвоєно звання заслуженого працівника народної освіти України.

З жовтня 2011 року кафедру очолює доктор технічних наук, професор, керівник Інформаційного комп'ютерного комплексу університету **Бабенко Тетяна Василівна.**

З грудня 2012 року кафедра носить нову назву **безпеки інформації та телекомунікацій (БІТ).**

Секція «Інформаційна безпека»

Голова секції: д.т.н., професор кафедри безпеки інформації та телекомунікацій Бабенко Т.В.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Масальська О.О.

УДК 65.011.3

ПРОБЛЕМИ СТРАХУВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ

Горошко Тетяна Сергіївна, Тимофєєв Дмитро Сергійович
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна
http://bit.nmu.org.ua, E-mail: tatyanagoroshko@mail.ru

Страхування інформаційних ризиків розвивається набагато повільніше, ніж інші сфери страхування, і не задовольняє потреб сучасності. У доповіді описано основні причини такого становища та запропоновані шляхи вирішення деяких з проблем.

Ключові слова – страхування; інформаційний ризик; оцінка загроз.

ВСТУП

Кожен день у світі відбуваються тисячі кібер-атак із застосуванням сотень різноманітних алгоритмів, тому навіть постійне вдосконалення систем захисту не надає достатнього рівня захищеності інформаційних активів. У більшості реальних систем захист знаходиться на крок позаду атаки. Такий стан речей закономірний: абсолютна безпека можлива хіба що за повної відсутності інтересу зловмисників до об'єкту захисту.

Найвідомішою успішною кібер-атакою 2014-го року став злом комп'ютерів кіностудії «Sony Pictures», через що розповсюдилися персональні дані працівників студії, її бухгалтерська звітність та інша конфіденційна інформація. Також сильного удару по престижу зазнала американська страхова компанія «Anthem», де через хакерську атаку стався витік персональних даних 80 мільйонів чоловік.

Не дивно, що в минулому році значно зріс попит на страхування інформаційних ризиків, компанії світу витратили в загальній сумі 2,5 мільярда доларів, рекордний показник. Але за прогнозами аналітиків 2002 року ця цифра повинна була би бути досягнута ще у 2005! Що ж так сповільнює розвиток цієї сфери страхування? Чому в Україні послуги страхування інформаційних ризиків досі не існує?

МЕТОДИКА ДОСЛІДЖЕННЯ

У процесі дослідження були порівняні публікації українських та закордонних експертів зі страхування інформаційних ризиків, а також досліджений досвід іноземних компаній у цій сфері (як страхувальників, так і страховиків).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Оцінка можливих загроз. В Україні перелік можливих загроз, їх критичність та вірогідність для підприємства визначає експерт, опираючись на куцу статистику, життєвий досвід та здоровий глузд. Експерту з-за кордону допоможе хіба що краща статистика.

2. Відсутність інформації про новітні розробки та загрози. Інформаційна безпека – важлива складова національної безпеки, тому багато розробок у цій сфері засекречено. Кожна країна намагається налагодити виробництво власної захисної техніки, якій зможе довіряти. Це значно впливає на ціну такої техніки – кожна одиниця робиться на замовлення. Зрозуміло, що звичайне підприємство не може собі дозволити систему захисту, яка, наприклад, функціонує в державних органах, де обробляється секретна інформація.

Що однією вагомою проблемою є неможливість захисту від вразливості «нульового дня», тобто вразливості програмного коду, яка стала публічно відомою до того, як розробник їх виправив.

3. Взаємопов'язаність інформаційних ризиків. Як не дивно, на захищеність підприємства впливає не тільки його власна система захисту, а і системи захисту інших підприємств (партнерів, філіалів, конкурентів тощо):

- злочинник, що заволодів комп'ютерною мережею одного підприємства, може заволодіти і мережею іншого підприємства, якщо вони взаємопов'язані.
- якщо злочиннику відомий спосіб проникнути в мережу одного підприємства, то він аналогічним чином може проникнути в мережі інших підприємств, що може призвести до події типу «чорний лебідь» - масової непередбачуваної, але критичної події (катастрофи). Страхова фірма буде вимушена надати страхові виплати усім постраждалим фірмам, що призведе до її банкрутства. Найкращим прикладом події «чорний лебідь» є «проблема Y2K» - при переході у нове, XXI століття, багато комп'ютерів мали формат дати «01.01.91», перші ж дві цифри року за замовченням залишилися «19». Тому тоді не дивно було побачити табло з датою «1900», або навіть бухгалтерську звітність столітньої давнини. По деяким оцінкам, на виправлення «проблеми Y2K» в США було витрачено 300 мільярдів доларів.
- злочинник серед усіх підприємств для атаки буде обирати підприємство з найгіршою системою захисту, що також впливає на розподіл вірогідності загроз.

4. Оцінка ефективності системи захисту. Не існує єдиного способу оцінки захищеності підприємства. Українське законодавство у цьому випадку пропонує побудову комплексної системи захисту інформації та визначення рівню гарантій. Побудова, сертифікація та обслуговування комплексної системи захисту коштує досить значну суму, яку не зможуть собі дозволити малі та більшість середніх підприємств.

Допомогти оцінити ефективність захищеності об'єктів інформаційної діяльності підприємств та відповідність системи захисту міжнародним стандартам можуть програмні продукти: Digital Security Office (Росія), RedCheck (Росія), RM Studio (США) та інші. Експерту достатньо відповісти на низку запитань та відтворити у програмі систему захисту, а усе інше підрахує програма. Недоліком є те, що усі програми ґрунтуються на різних моделях і тому дають різні результати. Також на підприємстві можуть використовуватись рішення з захисту інформації, які у програмі не передбачені.

5. Зменшення коштів на власний захист. Передаючи ризик страховій компанії, підприємство буде витрачати менше коштів на власну систему захисту. Це зумовлено тим, що частина виділених для захисту інформації коштів піде на страхування. Крім того, власник інформації може не захотіти ефективно організовувати захист, якщо йому вигідніше буде отримати страхові виплати, що повертає нас до проблеми пункту 4.

6. Незацікавленість розробників захисту. Розробники комерційних систем захисту насправді незацікавлені у розробці ідеального захисту, оскільки доки існують загрози, доти вони отримують прибуток. Хоча це не доведено, багато людей впевнені, що антивірусні компанії спонсорують створення комп'ютерних вірусів.

Які ж **рішення** можливі, щоб страхування було прийнятним і для страхувальника, і для страховика? За досвідом іноземних підприємств можна вивести деякі принципи:

1. Страхова компанія має наполягати, щоб на підприємстві існувала система менеджменту інформаційних ризиків. Так страхувальники можуть ідентифікувати ризики і приймати практику управління ризиками, щоб полегшити процес пошуку правильної захисту за правильну ціну, оптимізуючи перестрахування.

2. Щодо інформаційних ризиків, найкраще страхувати лише критичні загрози. Тобто підприємство отримає виплати, якщо його втрати перевищать деяку межу. Так підприємство не буде нехтувати власною системою захисту, і одночасно відхилення його ризиків від норми зменшиться, опинившись в зоні комфорту.

На жаль, моделі розрахунку платежів для подібного захисту орієнтовані на частоту реалізації ризиків 1 раз в 200 років, що підходить для землетрусів, потопів, пожеж, але навряд задовольнить інформаційну сферу. Тому можна математично створити "кібер-індекс" таким же чином, як погодні і фондові індекси, що з'являються в макроекономічних моделях і представляють взаємозв'язок ринкового ризику з іншими ризиками підприємства. Цей кібер-індекс може бути створений за шаблонами моделей кібер-катастроф та інших даних, а потім використовуватися як порогове значення для прийняття ризику.

3. Для страхування інформаційних ризиків можна використати компанію спеціального призначення (SPV). Цей підхід перенесення ризиків використовується в поєднанні з капіталами ринкових інвесторів і спонсорів, і він схожий на інвестиції в облігації катастроф, які захищають країни від ризику землетрусів. Головна ідея такого страхування - створення компанії спільно з урядом і приватним виробництвом, щоб оплатити претензії в разі глобальної або непередбачуваної, але критичного події (події «чорний лебідь»). Хоча дані взаємини є дуже ефективними, такі компанії часто мають тривалість життя в 10 років, а для перенесення інформаційних ризиків кращим буде коротший термін.

4. У страхуванні природних катастроф також використовуються дворічні поліси, що називають «колиска», які управляються страховою компанією. Інвестори вкладаються в ризики через рейтингові хедж-фонди. Якщо страхова подія не відбулося у встановлені терміни, інвестори отримають свої гроші назад з відсотками.

Такий підхід стане найкращим для невеликих підприємств. Це зробить страхування інформаційних ризиків частиною портфеля невзаємопов'язаних інвестицій.

ВИСНОВКИ

В результаті проведених досліджень було встановлено, що для розвитку ринку страхування інформаційних ризиків ще потрібен час, і навряд він з'явиться в Україні у цьому десятилітті. Потрібно вдосконалювати моделі та методи страхування, що будуть задовольняти саме інформаційну сферу. Тоді підприємства почнуть довіряти цьому виду страхування і будуть використовувати його як зручний інструмент управління ризиками.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Schwartz, Galina; Bohme, Rainer. «Modeling Cyber-Insurance». In Proceedings of WEIS, 2010.

2. «Mitigating cyber risk for insurers. Part 2: Insights into cyber security and risk», Ernst & Young, 2014.

3. Електронна енциклопедія «Вікіпедія» http://en.wikipedia.org/wiki/Cyber-Insurance.

УДК 004.056

РЕКОМЕНДАЦИИ ПО ПРОТИВОДЕЙСТВИЮ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ НА ПРЕДПРИЯТИИ

Богиня И.Г.[1], Мешков В.И.[2]
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: big94@ua.fm[1], local@i.ua[2]

В данной статье рассматриваются основные методы противодействия распространённым уязвимостям действующих ИС, позволяющих инсайдерам путем несанкционированного доступа к аппаратным и программным средствам системы нарушать свойства обрабатываемой информации.

Ключевые слова – методы и средства защиты информации; противодействие инсайдерской деятельности.

ВСТУПЛЕНИЕ

Согласно отчета украинской компании «СБК» (компании-аудитора ИБ, а также поставщика систем защиты от утечек информации), каждая пятая компания в Украине несла убытки от кибератак, более 70% компаний имеют крайне неэффективную антивирусную защиту, а большинство сотрудников, ответственных за работу с электронными счетами, слабо представляют способы защиты от несанкционированного доступа к этим счетам.

К сожалению, одним из уязвимых мест любой системы всегда остается человек. Работодатель не может быть уверен в полной лояльности и порядочности своих сотрудников. В процессе проектирования систем защиты часто не учитываются кажущиеся незначимыми особенности построения, которые, тем не менее, могут сыграть решающую роль в вопросах защиты информации.

ОСНОВНАЯ ЧАСТЬ

Приведем некоторые практические рекомендации по противодействию инсайдерской деятельности на предприятии:

1. Действенным, но, тем не менее, не всегда используемым решением в области защиты информации, является контроль доступа в помещение, где находится какой-либо узел ИС. Получение программного доступа там, где это не предусмотрено – задача, решение которой под силу лишь квалифицированным пользователям. С другой стороны, кража устройства физически доступна почти каждому.

2. При создании домена чаще всего автоматически создаются две учетные записи – гостя и администратора с соответствующими именами. Для осложнения подбора входных данных к учетной записи администратора для получения обширных полномочий в системе, следует переименовать запись администратора.

3. Стоит отключить возможность использования личных внешних носителей информации сотрудников компании, т.к. по умолчанию во многих ОС включена функция запуска с носителя файла autorun.inf при подключении внешнего устройства к системе. Данный файл мог быть модифицирован злоумышленником: к примеру, в файл могли быть внедрены скрипты, повышающие полномочия пользователя в системе до администратора.

4. В случае, когда запрещено использование внешних носителей информации, утечка может произойти через каналы электронной почты. Необходимо ограничить список лиц, которые могут писать внешним пользователям.

5. Используя прокси-сервер, необходимо запретить использование облачных хранилищ, а также запретить использование распространенных протоколов передачи файлов таких, как FTP для недопущения загрузки на вышеописанные сетевые ресурсы информации компании.

6. Эффективным решением, направленным на противодействие нарушению конфиденциальности и доступности информации и ресурсов, является использование систем обнаружения/предотвращения утечек информации (системы DLD/DLP) [3]. Существует два кардинально разных подхода по использованию вышеописанных систем:

- недопущение утечек любой информации (использование DLP-систем);
- допущение утечки определенной информации с последующим анализом цепочки получателей данной информации.

7. При выборе DLD/DLP-системы стоит учесть возможность шифрования файловых систем внешних носителей информации самой системой обнаружения/предотвращения утечек. Данная функция позволяет использовать только зарегистрированные устройства, выданные сотрудникам самой организацией. Это обеспечивает невозможность использования данных внешних устройств где-либо вне рассматриваемой ИС.

8. В случае, когда в ходе анализа угроз выявлена вероятная кража носителей информации, возможно использование Rights Management Services - технологии защиты документов на базе службы каталогов Microsoft Active Directory путем шифрования с применением ограничений доступа и лицензий доступа, позволяющей сохранять ограничения даже после загрузки и открытия файла пользователем. Технология требует поддержки со стороны клиентского ПО, применяемого для работы с документами; такую поддержку имеют Microsoft Office начиная с версий 2007 Enterprise, Professional Plus и Ultimate. AD RMS возможно использовать параллельно с другими технологиями такими, как

смарт-карты. Так же необходима поддержка со стороны клиентской ОС; в MS Windows 7/Vista/8/8.1 и Windows Server 2008/2012 включён клиент AD RMS [2].

9. В случае, когда пользователь системы имеет доступ к сетевому расположению с зашифрованными файлами (т.е. кража носителя информации не даст результата по причине отсутствия ключа расшифрования), то во время работы с файлом с помощью прикладного ПО сам файл хранится на клиентской системе как временный файл в незашифрованном виде. Из-за ошибок работы ОС и модулей памяти после выключения системы и даже после закрытия сеанса работы с приложением-редактором рассматриваемого файла, у пользователя есть возможность извлечь полезную информацию из случайно сохраненного временного файла. В качестве контрмеры, можно перенести все каталоги, где хранятся временные файлы, на сервер, к которому у пользователя не будет доступа, или переместить временные каталоги на RAM-диск, область в ОЗУ, определяемой ОС в качестве жесткого диска, содержимое которого будет уничтожено после выключения системы.

10. Исключить проблему НСД инсайдера к информации, хранящейся на клиентской машине, возможно путем виртуализации клиентских ОС. В данном случае, пользователь должен будет подключаться к удаленному рабочему столу, из-за чего на клиентской машине будет обрабатываться лишь принимаемое потоковое видео, а не сама информация, с которой работает сотрудник. Однако, использование стандартного протокола RDP не является наилучшим решением. По умолчанию, протокол RDP предоставляет общий буфер обмена для клиентской и виртуальной ОС, что является каналом утечки информации. Также, присутствует возможность подключения внешних дисков, с которых также можно скопировать данные. Решением данной проблемы является использование терминального сервера, контролирующего использование виртуальных рабочих столов, или использование таких протоколов, как PC-over-IP, предоставляющих только лишь потоковое видео и ничего более, перекрывая каналы утечки [1].

ЗАКЛЮЧЕНИЕ

Уровень эффективности вышеописанных методик напрямую зависит от того, насколько своевременно, квалифицированно, полно и комплексно они реализованы. Необходимо отметить, что при решении задачи противодействия инсайдерской деятельности ключевыми факторами успешности являются как уровень профессионализма специалистов, внедряющих данные методики, так и степень понимания руководством компании важности и необходимости принимаемых мер.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Михеев М. О. Администрирование VMware vSpere 5. М.: Буки Веди, 2012. - 505 с.
2. Р. Моримото, М. Ноэл, Г. Ярдени, О. Драуби, Э. Аббат, К. Амарис. Microsoft Windows Server 2012. Полное руководство. М.: Вильямс, 2013. – 1456 с.
3. Богиня Г.А. Тезисы доклада «Выявление инсайдеров: Практический опыт. Тонкости проведения служебных расследований с помощью аналитического модуля КИБ SI», г. Сочи, закрытая конференция по информационной безопасности.

УДК 004.75:004.056

ОСНОВНЫЕ УЯЗВИМОСТИ В СИСТЕМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Смирнов Арсений Евгеньевич
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: 148abc@gmail.com

В данной работе перечислены и описаны модели развертывания и предоставления пользователям услуг облачных вычислений. Проанализированы основные уязвимости, связанные с использованием систем облачных вычислений в корпоративной среде.

Информационная безопасность; облачные вычисления; виртуальная машина; уязвимость.

ВСТУПЛЕНИЕ

В организациях сегодня все активнее внедряются облачными вычислениями как инструментом экономии денег и повышения продуктивности. Однако распространение облачных вычислений вызывает проблемы безопасности у потребителей и у поставщиков облачных сервисов. Ключевой задачей для преодоления этих трудностей является определение основных угроз и разработка соответствующих контрмер.

МОДЕЛИ ПРЕДОСТАВЛЕНИЯ УСЛУГ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

На сегодняшний день существует несколько видов систем облачных вычислений (рис. 1), каждый из которых, из-за технологических и организационных особенностей, может включать разные методы защиты.

Частное облако — это модель, предназначенная для использования одной организацией, включающей несколько потребителей, возможно, клиентов и

подрядчиков данной организации. Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны, и оно может физически существовать как внутри, так и вне юрисдикции владельца. [1]

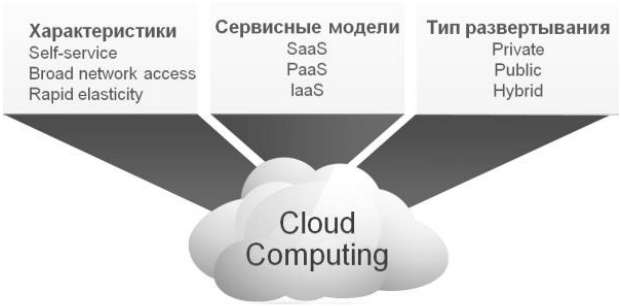


Рисунок 1. Ключевые составляющие облачных систем

Публичное облако — это инфраструктура, предназначенная для свободного использования широким кругом пользователей. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций.

Гибридное облако — это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанны между собой стандартизированными или частными технологиями передачи данных и приложений.

Общественное облако — вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики).

Кроме того, существует несколько моделей предоставления услуг, которые может использовать провайдер.

Программное обеспечение как услуга — модель, в которой потребителю предоставляется возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре и доступного из различных клиентских устройств или посредством тонкого клиента, или интерфейса программы. Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем или даже индивидуальных возможностей приложения осуществляется облачным провайдером. [1]

Платформа как услуга — модель, когда потребителю предоставляется возможность использования облачной инфраструктуры для размещения базового программного обеспечения для последующего размещения на нём новых или существующих приложений. Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем осуществляется облачным провайдером, за исключением разработанных или установленных приложений, а также, по возможности, параметров конфигурации среды (платформы).

Инфраструктура как услуга — модель, при использовании которой предоставляется возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, передачи данных и другими фундаментальными вычислительными ресурсами. Потребитель может контролировать операционные системы, виртуальные системы хранения данных и установленные приложения, а также набор доступных сервисов. [1]

Каждая модель имеет свои организационные и технические особенности, которые приводят к возникновению соответствующих уязвимостей.

УЯЗВИМОСТИ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ

Фактически задачу защиты облака можно разделить на две составляющие: обеспечение безопасности функционирования оборудования и обеспечение безопасности данных. Провайдер должен реализовать защиту своего аппаратно-программного комплекса от несанкционированного вторжения, модификации кода, взлома ИТ-системы, чтобы обеспечить защиту данных клиента. Клиент, в свою очередь, при необходимости размещения каких-либо важных и секретных данных, может использовать технологии шифрования для защиты ценной информации от несанкционированного доступа.

В процессе организации системы безопасности провайдер и клиент должны учитывать следующие основные уязвимости облачных систем:

1. Сложность контроля и управления облаками

Необходимо удостовериться, что все ресурсы облака инвентаризированы и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака. Это высокоуровневый тип уязвимостей, т.к. он связан с управляемостью облаком, как единой информационной системой и для него общую защиту нужно строить индивидуально. Для этого необходимо использовать модель управления рисками для облачных инфраструктур.

2. Трудности при перемещении обычных серверов в вычислительное облако

Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных. Однако виртуализация систем облачных вычислений и переход к облачным средам приводят к появлению новых угроз и уязвимостей.

Доступ через Интернет к управлению вычислительной мощностью — одна из ключевых характеристик облачных вычислений. В большинстве традиционных систем облачных вычислений доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

3. Динамичность виртуальных машин [2]

Высокоскоростная изменчивость внутренней

инфраструктуры сильно усложняет разработку целостной системы безопасности. Уязвимости операционной системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются не сразу, а через определенный промежуток времени (например, при восстановлении из резервной копии). В средах облачных вычислениях важно надежно зафиксировать определенный уровень защиты системы. При этом он не должен зависеть от текущего состояния используемых сегментов.

4. Уязвимости внутри виртуальной среды

Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным программным обеспечением высока. Риск для виртуальных систем также высок. Параллельные виртуальные машины увеличивает «атакуемую поверхность». Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

5. Бездействующие виртуальные машины

Когда виртуальная машина выключена, она подвергается опасности заражения. Для осуществления атаки достаточно доступа к хранилищу образов виртуальных машин через сеть. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение. В данном случае должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

6. Отсутствие периметра и разграничения сети

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине. Корпоративный брандмауэр как основной компонент для внедрения политики информационной безопасности и разграничения сегментов сети не в состоянии повлиять на серверы, размещенные в облачных системах. [2]

ЗАКЛЮЧЕНИЕ

Таким образом, защита данных – задача, решение которой ложится на плечи не только оператора, но и самого клиента. При этом в каждом отдельном случае могут использоваться свои методы защиты данных, которые будут отличаться в зависимости от вида используемых облачных сервисов. При продуманной стратегии и наличии достаточного потенциала современные технологии позволяют обеспечить в облачной среде практически любой уровень безопасности, вплоть до самых высоких требований к защите персональных данных.

ПЕРЕЧЕНЬ ИСТОЧНИКОВ

1. Cloud Computing. Benefits, risks and recommendations for information security; European Network and Information Security Agency; Rev.B – December 2012.

2. The Notorious Nine: Cloud Computing Top Threats; CLOUD SECURITY ALLIANCE; 2013.

УДК 65.012.8:658

МОДЕЛЬ PDCA ОПИС ЖИТТЄВОГО ЦИКЛУ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІБ

Дніпровський Олексій Павлович
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: alex93dnepr@gmail.com

В статті висвітлюється сценарний та опис життєвого циклу управління процесів згідно з моделлю PDCA.

Ключові слова – модель PDCA; життєвий цикл; процес управління інцидентами ІБ.

ВСТУП

У багатьох компаніях не завжди можливо простежити за зміною кількості та характеру інцидентів інформаційної безпеки - відсутня процедура управління інцидентами. Часто відсутність інцидентів не вказує на те, що система управління безпекою працює правильно, а означає лише, що інциденти не фіксуються або не визначаються. Також слід зазначити що управління інцидентами це не від'ємна складова загальної системи менеджменту інформаційної безпеки.[1]

ДОСЛІДЖЕННЯ

Визначення інциденту. У компанії відсутня методика визначення інцидентів, а співробітники не знають, які події є інцидентами. Це особливо важливо у випадку інцидентів інформаційної безпеки - вони не завжди заважають нормальній роботі. Наприклад, інцидентом безпеки буде залишення без нагляду на столі конфіденційних документів, на що ніхто може і не звернути уваги, а зловмисник (який може бути співробітником компанії) такі документи помітить.

Оповіщення про виникнення інциденту. Співробітники компанії часто не інформовані про те, кого і в якій формі слід ставити до відома при виникненні інциденту, - наприклад, не визначені ні форми звітів, ні перелік осіб, яким необхідно відправляти звіти про інциденти. Навіть якщо

співробітник помітить, що його колега забирає для роботи додому конфіденційні документи компанії, він не завжди знає, які дії слід робити в даній ситуації.

Реєстрація інциденту. Відповідальним особам (навіть якщо такі призначені) часто не надається методика реєстрації інцидентів - не існує спеціальних журналів їх реєстрації, а також правил і термінів заповнення.

Усунення наслідків і причин інциденту. У компаніях, як правило, відсутня документально зафіксована процедура, що описує дії, які необхідно виконати з метою усунення наслідків і причин інциденту. У першу чергу така процедура повинна передбачати, щоб заходи з усунення наслідків і причин інциденту не порушували процедури їх розслідування: усунення наслідків інциденту не повинно «замітати сліди», щоб неможливо було встановити винних в інциденті.

Розслідування інциденту. На етапі розслідування інцидентів основну роль грають: ведення журналів реєстрації подій, чіткий поділ повноважень користувачів, відповідальність за виконані дії - важливі докази того, хто брав участь в інциденті і які дії він виконував. На жаль, про розслідування інцидентів в компаніях часто просто забувають. Як тільки наслідки інциденту усунені і бізнес-процеси відновлені, подальші дії з розслідування інциденту і здійсненню коригувальних і превентивних заходів не виконуються.

Реалізація дій, що попереджають повторне виникнення інциденту. Як правило, якщо компанії було завдано якоїсь шкоди, то до винних у виникненні інциденту все ж застосовуються різні стягнення, однак внесення дисциплінарних стягнень не завжди підпорядковується затвердженими процедурами та інші дії щодо запобігання повторення інциденту виконуються теж не завжди.[4]

Управління інцидентами - одна з найважливіших процедур управління інформаційною безпекою. Насамперед, важливо правильно і своєчасно усунути наслідки інциденту, а також мати можливість проконтролювати, які дії були виконані для цього. Необхідно також розслідувати інцидент, що включає визначення причин його виникнення, винних осіб і конкретних дисциплінарних стягнень. Далі, як правило, слід виконати оцінку необхідності дій щодо усунення причин інциденту, якщо потрібно - реалізувати їх, а також виконати дії щодо попередження повторного виникнення інциденту. Крім цього, важливо зберігати всі дані про інциденти інформаційної безпеки, так як статистика інцидентів інформаційної безпеки допомагає усвідомлювати їх кількість і характер, а також зміна в часі. За допомогою інформації про статистику інцидентів можна визначити найбільш актуальні загрози для компанії і, відповідно, максимально точно планувати заходи щодо підвищення рівня захищеності інформаційної системи компанії.

Тут розглянуті тільки основні елементи процедури управління інцидентами інформаційної безпеки, але і їх достатньо, щоб зрозуміти загальний принцип управління інцидентами.[2]

Розглянемо практичні рекомендації з даного питання. При створенні системи управління інцидентами критично важливо, щоб всі співробітники компанії розуміли, що забезпечення інформаційної безпеки в цілому і управління інцидентами зокрема є основними бізнес-цілями компанії.

Потім слід розробити необхідні нормативні документи з управління інцидентами. Як правило, такі документи повинні описувати:

1. Визначення інциденту інформаційної безпеки, перелік подій, що є інцидентами (що в компанії є інцидентом).
2. Порядок оповіщення відповідальної особи про виникнення інциденту (необхідно визначити формат звіту, а також відобразити контактну інформацію осіб, яких слід оповіщати про інцидент).
3. Порядок усунення наслідків і причин інциденту.
4. Порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору та збереження доказів).
5. Внесення дисциплінарних стягнень.
6. Реалізація необхідних коригувальних і превентивних заходів.

Визначення переліку подій, що є інцидентами, - важливий етап розробки процедури управління інцидентами. Слід розуміти, що всі події, які не увійдуть до зазначеного переліку, будуть розглядатися як штатні (навіть якщо вони несуть загрозу інформаційній безпеці). Зокрема, інцидентами інформаційної безпеки можуть бути:

- відмова в обслуговуванні сервісів, засобів обробки інформації, обладнання;
- порушення конфіденційності та цілісності цінної інформації;
- недотримання вимог до інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації);
- незаконний моніторинг інформаційної системи;
- шкідливі програми;
- компрометація інформаційної системи (наприклад, розголошення пароля користувача).[2]

Як приклад інцидентів можна привести такі події, як неавторизоване зміна даних на сайті компанії, залишення комп'ютера незаблокованим без нагляду, пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти. У загальному випадку інцидент інформаційної безпеки визначається як одиничне, небажане або несподівана подія інформаційної безпеки (або сукупність таких подій), яке може скомпрометувати бізнес-процеси компанії або загрожує її інформаційної безпеки.[3]

Важливо відзначити, що процедура управління інцидентами тісно пов'язана з усіма іншими процедурами управління безпекою в компанії. Оскільки інцидентом, в першу чергу, є недозволене подія, воно повинно бути кимось заборонено, отже, необхідна наявність документів, чітко описують всі дії, які можна виконувати в системі і які виконувати заборонено. Наприклад, в одній з компаній співробітник зберігав на мобільному комп'ютері

конфіденційні відомості компанії без застосування засобів шифрування. Після роботи він забрав комп'ютер додому і забув його в машині, яку залишив під вікнами будинку, а вночі машину зламали, і комп'ютер був вкрадений. Зловмисники отримали доступ до конфіденційної інформації компанії і могли продати її конкурентам. Крім цього, на комп'ютері зберігалася цінна інформація, яка не була зарезервована на іншому носії. Такий інцидент міг статися в результаті того, що в компанії не були розроблені процедури поводження з мобільними комп'ютерами та зберігання на них інформації. Винос комп'ютера за межі офісу компанії, відсутність засобів шифрування і резервного копіювання інформації - можливі порушення, а отже, причини інцидентів. Однак поки документально не зафіксовано, що це порушення (тобто у відповідних документах не описано, що це заборонено), співробітника неможливо притягнути до відповідальності і запобігти повторне виконання неправомірних дій.

ВИСНОВОК

Важливо, щоб були налагоджені такі процедури, як моніторинг подій, своєчасне видалення не використовуваних облікових записів, контроль і моніторинг дій користувачів, контроль над діями системних адміністраторів та ін. В одній з компаній був зафіксований наступний інцидент: при звільненні з роботи системний адміністратор вкрав розробляється в компанії програмний продукт і передав його конкурентам, які випустили програму на ринок під своїм товарним знаком. Крім цього, він вніс зміни в інформаційну систему, в результаті яких після його відходу функціонування певних її компонентів було порушено. Залучити адміністратора до відповідальності в даному випадку виявилося неможливо, тому що, по-перше, не виконувалася реєстрація його дій, по-друге, адміністратор міг видалити всі докази своїх неправомірних дій і, по-третє, не була налагоджена процедура збору доказів про інцидент. Крім цього, в компанії просто не знали, як слід чинити в таких випадках (наприклад, можна було звернутися в спеціалізовану компанію з розслідування інцидентів або подати заяву в суд).

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO 27001:2013 Information technology - Security techniques - Information security management systems
2. http://www.hbc.ru/news/analytics/security/133.html
3. ISO / IEC TR 18044:2004 Information technology -- Security techniques -- Information security incident management
4. Инженерное проектирование систем информационной безопасности, http://193.124.209.204/default.aspx?db=book_permyakov&int=VIEW&el=1859&templ=I206

УДК:004.056:65.012.8

ЗАЩИТА ГОСТИНИЧНОГО БИЗНЕСА ОТ КИБЕРПРЕСТУПНОСТИ

Бараник Эдуард Линарович, Галушко Светлана Алексеевна
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: kurmanaeve@gmail.com

Защита персональных данных постояльцев гостиниц от киберпреступников. Распространенные методы атак и их минимизация.

Ключевые слова – киберприступник, защита, информационные технологии, гостиничный бизнес, риски.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСТИНИЧНОГО БИЗНЕСА

В информационных системах гостиничного бизнеса обрабатываются конфиденциальные данные клиентов и сотрудников, включая почтовые адреса, номера контактных телефонов, адреса электронной почты, данные кредитных и дебетовых карт. По этой причине гостиничный сектор, как и многие другие виды бизнеса, остается одной из самых желанных мишеней киберпреступников: на него приходится 15% от общего числа случаев утечки данных. Существует целый ряд разновидностей мошенничества, которым подвержена гостиничная индустрия. Как правило, эти мошенничества совершаются через Интернет или электронную почту. Мошенничество с кредитными картами – один из наиболее распространенных видов преступлений, с которым сталкиваются предприятия, обрабатывающие финансовые данные клиентов. Чтобы украсть конфиденциальную информацию, хакеры осуществляют атаки класса «человек посередине» (man-in-the-middle), позволяющие перехватить трафик между клиентскими машинами и серверами. Для получения несанкционированного доступа к конфиденциальным данным злоумышленники также используют технику фишинга – нацеленную рассылку фальшивых писем от имени легитимных организаций. Фишинговые атаки приводят к невольному раскрытию конфиденциальной информации сотрудниками и заражению компьютеров троянскими программами. Другая часто используемая технология атак – это внедрение SQL-кода, когда база данных организации взламывается через корпоративный сайт. При этом эксплуатируются уязвимости программного обеспечения веб-сайта, позволяющие злоумышленнику с помощью специального запроса, вводимого через веб-форму, изменить или прочитать

информацию, содержащуюся в базе (например, пароли или данные кредитных карт).[1]

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ МЕТОДЫ АТАК

Одна из часто используемых хакерских техник – это атаки через Интернет на приложение, к которому имеется удаленный доступ. Гостиничный сектор является излюбленной мишенью для киберпреступников, поскольку организации этой отрасли используют многочисленные внутренние или внешние каналы связи с сотрудниками и ИТ-специалистами. Такие системы часто реализованы без парольной защиты или с легко угадываемыми паролями и, значит, плохо защищены от внешних атак. Киберпреступники с помощью ботнетов заражают компьютеры, а затем дистанционно управляют инфицированными машинами в целях совершения преступной деятельности. Используя такие компьютеры, киберпреступники могут проводить DoS-атаки, делая веб-сайты туристических компаний и отелей недоступными для легитимных пользователей. Также хакеры компрометируют веб-серверы и размещают на них вредоносный контент, что позволяет заражать компьютеры клиентов, посещающих туристические веб-сайты для выполнения онлайн-бронирования и других задач. Это ведет к потере репутации туристической организации. По данным аналитической компании Forrester Research, примерно в 85% случаев утечка информации происходят из-за действий сотрудников пострадавшей организации (инсайдеров). Инсайдерский инцидент может быть результатом небрежности сотрудника, его несанкционированного доступа к конфиденциальной информации, кражи ноутбука, слабого управления идентификационными данными и т.д. В результате успешной инсайдерской атаки возможны резкое снижение доходов компании, юридические последствия, а также ухудшение имиджа бренда [1].

МИНИМИЗАЦИЯЬ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСТИНИЧНОГО СЕКТОРА

- Использование закрытых сетей (без доступа к внешним сетям за исключением интрасети и внутренней почты). Особое внимание следует уделить обеспечению закрытости внутренних Wi-Fi-сетей отеля;
- Ограничение использования сотрудниками внешних устройств, таких как флэш-карты и USB-модемы;
- Соблюдение норм и стандартов информационной безопасности, например, стандарта безопасности данных в индустрии платежных карт PCI-DSS;
- Централизованное управление ИТ-инфраструктурой и ИТ-безопасностью, соблюдение политик информационной безопасности, в том числе своевременная установка исправлений и патчей, регулярное обновление антивирусных баз, ограничение доступа к ресурсам и контроль приложений[2].

НЕОБХОДИМОСТЬ ОБЕСПЕЧЕНИЯ ИТ-БЕЗОПАСНОСТИ

Большинство руководителей предприятий гостиничного сектора понимают важность поддержания высокого уровня информационной безопасности, с ростом киберпреступности степень этой осведомленности растёт, и руководители гостиничных компаний стали с большей ответственностью подходить к обеспечению[2].

ВЫВОД

Необходимо правильно выбрать решение информационной безопасности, удовлетворяющее всем потребностям организации. Оно должно обеспечивать многоуровневую продуманную защиту в режиме реального времени от любых возможных угроз. Решение должно иметь эффективный сканер, определяющий даже уязвимости нулевого дня в приложениях, сети и операционной системе. Необходимо, чтобы такое решение включало брандмауэр, который эффективно фильтрует входящий и исходящий трафик сети. Также нужна функция контроля доступа к сети для предотвращения подключения неавторизованных устройств. Кроме того, выбранное решение должно производить мониторинг сети в режиме реального времени, идентифицировать вредоносные программы и уведомлять администратора об их появлении, предотвращать распространение вредоносного программного обеспечения по сети[3].

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Безопасность в гостинице. http://www.referatnatemu.com/id=6023_часть=2

2. Информационная безопасность в гостиницах: как это работает? http://devicebox.ru/informacionnaya-bezopasnost-v-gostinicax-kak-eto-rabotaet/

3. Обеспечение информационной безопасности в гостиницах. http://www.bezpeka.com/ru/lib/sec/tematic-publications/personal-security/art1226.html

УДК 004.91:65.012.8

СПЕЦИФИКАЦИЯ ПОСТРОЕНИЯ ДОКУМЕНТА ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Поспелова Екатерина Викторовна, Тимофеев Дмитрий Сергеевич
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: kate_pospelova@ukr.net

В статье ставится задача рассмотреть предназначение политики безопасности, а также определить главные проблемы, решаемые с ее помощью. Основное внимание посвящено структуре политики безопасности и ее содержанию. Статья рассматривает область применения политики безопасности, также сферу ее действия.

Ключевые слова – политика безопасности (ПБ); информационная безопасность (ИБ); структура; описание проблемы; ЛВС.

ВСТУПЛЕНИЕ

В решении задачи разработки политики безопасности информации необходимо уделить внимание таким аспектам, как определение ее понятия, описание существующих проблем, выделение области применения и разработка детальной структуры.

ОСНОВНЫЕ ПОНЯТИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ

Под политикой безопасности информации (далее политика безопасности, ПБ) организации (англ. *organizational security policies*) понимают совокупность документированных управленческих решений, руководящих правил, процедур, практических приемов, а также принципов, которые направленны на защиту, урегулирование управления и распределение ценной информации с ассоциированными ресурсами. ПБ можно определить, как стратегию управления в области информационной безопасности, построенную на основе анализа рисков, а также меру внимания и количество ресурсов, которые считает целесообразным выделить руководство [1].

Специфичность структуры политики безопасности зависит от определенных факторов, а именно:

• от конкретной технологии обработки информации;

• от используемых технических и программных средств;

• от расположения организации.

ОПИСАНИЕ ПРОБЛЕМЫ

Как правило, в локальной вычислительной сети (ЛВС) циркулирует критически важная информация. Каждый ПК (персональный компьютер), подсоединенный к ЛВС, нуждается в мероприятиях по защите. Это связанно с тем, что локальная сеть дает возможность всем ее пользователям использовать данные и программы совместно, что, в свою очередь, повышает уровень угрозы безопасности. Именно документ, описывающий структуру ПБ, призван продемонстрировать сотрудникам организации важность защиты сетевой среды, описать их роль в обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в сети.

ОБЛАСТЬ ПРИМЕНЕНИЯ

В сферу действия такой ПБ включены все программные, аппаратные и информационные ресурсы, которые входят в ЛВС данного предприятия. Политика безопасности локальной сети может быть ориентирована не только на ресурсы, а также и на людей, работающих с сетью, в том числе и на пользователей, субподрядчиков и поставщиков (если таковые имеют место).

СТРУКТУРА ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Политика безопасности организации, а именно соответствующий документ высокоуровневой политики, который, в свою очередь, поддерживается документами специализированных политик и процедур безопасности, должен иметь доступную и легко понимаемую структуру. Для большинства организаций политика безопасности абсолютно необходима, так как именно она определяет и устанавливает отношение организации к обеспечению безопасности, а также необходимые действия по защите своих ресурсов и активов.

Как правило, ПБ организации (документ, представляющий методологическую основу практических мер и процедур по реализации обеспечения безопасности) содержит:

• базовую политику безопасности (включающую определение разрешенных и запрещенных действий, а также необходимые средства управления);

• специализированные политики безопасности;

• процедуры безопасности;

•руководство по архитектуре безопасности (описывающее реализацию механизмов безопасности в компонентах архитектуры, используемых в сети организации) [2].

Методология разработки политики безопасности включает в себя следующие работы:

- разработка концепции безопасности информации в автоматизированной системе;
- анализ рисков;

- определение методов и средств защиты, а также требований к мерам защиты;
- выбор основных решений по обеспечению безопасности информации;
- организация выполнения восстановительных работ и обеспечения непрерывного функционирования АС;
-документальное оформление политики безопасности [3].

Основные данные, содержащиеся в ПБ организации можно разбить на более детальные группы сведений:

1.Основные положения информационной безопасности (ИБ).

2. Область применения.

3. Цели и задачи обеспечения ИБ.

4. Распределение ролей и ответственности. Общие обязанности должностных лиц.

Рассмотрим вышеупомянутые данные на примере гипотетической локальной сети.

Основные положения ИБ: определяют важность и общие проблемы безопасности, а также направления их решений, нормативно-правовые основы и роль сотрудников.

Область применения: включает в себя основные активы (программно-аппаратное, информационное обеспечение автоматизированной системы (АС), персонал) и подсистемы АС, которые подлежат защите.

Цели, задачи: аспекты, вытекающие из функционального назначения предприятия. В роли цели/задачи обеспечения ИБ могут выступать следующие требования:

• обеспечение уровня безопасности, который соответствует нормативным документам предприятия;

• следование экономической целесообразности в выборе защитных мер;

• обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;

• обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;

• выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

*Распределение ролей и ответственности, общие обязанности: н*а каждом предприятии существуют соответствующие должностные лица, а также сами пользователи сети, которые несут ответственность за реализацию поставленных целей и задач. Сотрудников, выступающих в роли ответственных лиц можно разделить на группы:

1. Руководители подразделений. В их обязанности входят контакты с пользователями и доведение до них положений ПБ.

2. Администраторы ЛВС. Несут ответственность за непрерывное функционирование сети и реализацию технических мер, которые необходимы для внедрения в предприятие ПБ.

3. Администраторы сервисов. Данная группа лиц отвечает за конкретные сервисы, управлениями правами доступа пользователей, а также за построение защиты в соответствии с ПБ.

4. Пользователи. Используют локальную сеть только в соответствии с установленной ПБ и, в случае необходимости, извещают руководство обо всех нестандартных ситуациях. [4]

МЕТОДЫ ОЦЕНКИ

Выделяются две основные системы оценивания текущей ситуации в области ИБ предприятия («исследование снизу-вверх» и «исследование сверху вниз»). Рассматривая первую систему, можно отметить, что основываясь на всех известных видах атак и применяя их на практике, существует возможность проверить реальность осуществления атаки определенного вида от возможного злоумышленника. Что касаемо системы «исследование сверху вниз», она представляет собой детальный анализ всей существующей схемы хранения и обработки информации, а именно необходимых в защите информационных объектов и потоков, изучение текущего состояния ИБ, классификация всех информационных объектов на классы в соответствии с ее КЦД (конфиденциальностью, целостностью и доступностью).

ВЫВОД

Применение политики безопасности на предприятии будет считаться эффективным, в случае, если удовлетворены последующие условия:

• При запуске новых систем и проектов должны соблюдаться условия имеющейся ПБ и процедуры ее разработки.

• В случаях утверждений новых ПБ, каждую систему следует проверять на соответствие утверждаемым политикам.

• Каждая функционирующая ПБ на предприятии должна соответствовать требованиям организации.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. НД ТЗИ 1.1-003-99, “Терминология в сфере защиты инфоормации в компьютерных системах от несанкционированного доступа”

2. Кормич Б. А. Организационно-правовые основы политики информационной безопасности Украины: Автореф. дис. д-ра юрид. наук: 12.00.07. — Х.: НХУ Украины, 2004

3. НД ТЗИ 1.4-001-2000, “Положение о службе защиты информации в автоматизированных системах”

4. Информационная политика Украины: состояние и перспективы // Вестник Книжной палаты – 1999 р. - № 5

УДК:004.056:65.012.8

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ ЯК ПРОТИДІЯ ІНФОРМАЦІЙНИМ ВІЙНАМ

Аветисьян Арсен Ваграмович, Гулина Ирина Григорьевна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: arximed.pro@gmail.com

Аналіз головних складових інформаційної безпеки держави. Проблема інформаційної безпеки має давнє походження і стала особливо важливою у наш час, коли використання інформаційних технологій відбувається вже практично у всіх сферах нашого життя.

Ключові слова – інформаційна безпека, держава, інформаційна війна.

ВСТУП

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій.

ОСНОВНА ЧАСТИНА

Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення. Країни, які не можуть забезпечити власну інформаційну безпеку, стають неконкуренто спроможними і, як наслідок, не можуть брати участь у боротьбі за розподіл ринків та ресурсів. Можна стверджувати, що зникнення великих держав відбувалося не в останню чергу через неспроможність ефективного управління на власній території та невідповідність інформаційної структури новим умовам існування. Отже, незаперечним є те, що в будь-якій розвиненій країні має існувати система забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені законодавчо. Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів тощо. Рішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації. Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як: розроблення теоретичних основ забезпечення безпеки інформації; створення системи органів, відповідальних за безпеку інформації; вирішення проблеми керування захистом інформації і її автоматизації; створення нормативно-правової бази, що регламентує рішення всіх задач забезпечення безпеки інформації; налагодження виробництва засобів захисту інформації; організація підготовки відповідних фахівців та ін. Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності як: захист та обмеження обігу інформації; захист інформаційної інфраструктури держави; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; попередження інформаційного тероризму та інформаційної війни [1].

Існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. З одного боку, це самостійний елемент національної безпеки будь-якої країни, а з іншого - інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д. Одним з найбільш повних визначень інформаційної безпеки можна вважати наступне: це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації. Це визначення тією чи іншою мірою охоплює практично всі сфери інформаційної взаємодії суб'єктів держави.

Захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії. Серед головних складових інформаційної безпеки держави виділяють: обсяг інформаційного продукту, що виробляється в державі і державою; здатність мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати розвитком вироблення та розповсюдження інформації; можливість доступу народонаселення до усіх можливих інформаційних джерел, а також відкритість більшості з них. [2]

На національному рівні інформаційна безпека держави розглядається як система заходів, спрямованих на недопущення несанкціонованого

доступу до інформації, її модифікації та порушення цілісності. Вона включає: захист політичних, державних і громадських інтересів; захист моральних цінностей; заборона інформації, яка містить ідеї агресивної війни, насилля, дискримінації та посягання на права людини [4].

Відповідно до вищеназваних принципів і положень забезпечення інформаційної безпеки держави вимагає рішення наступних ключових проблем: розвиток науково-практичних основ інформаційної безпеки, що відповідають сучасній геополітичній ситуації та умовам політичного і соціально-економічного розвитку держави; формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, у тому числі розробка реєстру інформаційного ресурсу, регламенту інформаційного обміну для органів державної влади, підприємств, нормативного закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки; розробка механізмів реалізації прав громадян на інформацію; формування системи інформаційної безпеки, що є складовою частиною загальної системи національної безпеки країни; розробка сучасних методів і технічних засобів, що забезпечують комплексне рішення задач захисту інформації; розробка критеріїв і методів оцінки ефективності систем і засобів інформаційної безпеки і їх сертифікація; дослідження форм і способів цивілізованого впливу держави на формування суспільної свідомості; комплексне дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією. На національному рівні інформаційна безпека держави розглядається як система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, її модифікації та порушення цілісності. Вона включає: захист політичних, державних і громадських інтересів; захист моральних цінностей; заборона інформації, яка містить ідеї агресивної війни, насилля, дискримінації та посягання на права людини [3,5].

ВИСНОВОК

Вищесказане дозволяє зробити висновок, що необхідний рівень інформаційної безпеки держави забезпечується цілим комплексом політичних, економічних, організаційних та інших заходів, які допомагають реалізації інформаційних прав та інтересів держави і її суб'єктів.

Отже, наукове осмислення комплексу проблем, пов'язаних з розробкою та втіленням у життя державної політики в інформаційній сфері, сьогодні набуває особливого значення, оскільки їх розв'язання сприятиме розвитку в Україні інформаційного суспільства і, таким чином – забезпеченню національної та інформаційної безпеки нашої держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соснін О.В. Інформаційна політика України: проблеми розбудови [Електронний ресурс] – Режим доступу: http://www.niisp.gov.ua/vydanna/panorama
2 Інформаційна потужність держави, як складова національної безпеки. [Електронний ресурс] – Режим доступу: http://propolis.com.ua
3. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. [Електронний ресурс] – Режим доступу: http://www.viche.info
4. Закон України Про основи національної безпеки України // Відомості Верховної Ради. – 2003. – № 39. – Ст. 351.
5. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua
6. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Фонд «Мир», 2003. – 640 с.

УДК 351.862

СИСТЕМА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Демченко Дмитро Геннадійович
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: 3ddemkin@gmail.com

Використання інформаційної безпеки в Україні у розрізі інформаційної обороноздатності країни

Ключові слова – інформаційна безпека, національна безпека

ВСТУП

Питання «безпеки» на початку двадцять першого століття набуло більш загального змісту. Окрім загальноприйнятої військової, військово-політичної галузей, воно розповсюдилось на сфери економічних, соціальних, екологічних, культурних, правових та інформаційних відносин. До того ж, двадцять перше століття утворило деякі інші типи небезпеки: продовольчу, енергетичну, епідеміологічну, демографічну, що зумовлено утворенням відповідних програм забезпечення безпеки як державного, так і вищих рівнів.

В Україні особливо гостро постає питання забезпечення національної безпеки, це обумовлено існуванню таких проблем як: необхідність утворення умов котрі сприяють задля майбутнього розвитку українського суспільства та держави вцілому; існування безперервної економічної кризи; зростання рівня корупції та злочинності; розширення загроз тероризму, обмеження конституційних прав і свобод людини в Україні та за її межами; безконтрольного розповсюдження зброї та наркотиків; забруднене довкілля; значне погіршення демографічної ситуації у

країні.

Забезпечення національної безпеки відбувається за умови пріоритетності державних інтересів, необхідності своєчасного вжиття дієвих заходів, які відповідають характеру і масштабам загроз цим інтересам, і ґрунтується на засадах правової демократичної держави.

ОСНОВНА ЧАСТИНА

При нинішньому розвитку української держави та розвитку інформаційних технологій у світі гостро постає питання гарантування саме інформаційної безпеки, тому що відсутність теоретично-правових досліджень проблем ролі та місця, повноважень та функцій органів державної влади у сфері забезпечення інформаційної національної безпеки України, питання правового урегулювання їх діяльності по забезпеченню національної безпеки, правових форм зв'язку з іншими суб'єктами цієї системи, сприяє зріст саме інформаційної злочинності, яка зазіхає передусім на інтереси країни.

Зокрема, вагоме значення теми пояснюється ще й тим чинником що необхідне наукове усвідомлення у контексті нинішньої державно-правової реформи шляхів удосконалення системи національних і правоохоронних структур та органів, з тим, щоби ця система могла своєчасно прилаштуватися до змін у суспільстві, насамперед якщо є ризик виникнення чи зростання деструктивних чинників у країні, зміна рівнів небезпеки загроз які вже існують і ступеня важливості пріоритетних інтересів України.

За умов жорстокої міжнародної боротьби головною ареною конкуренції у Всесвіті різноманітних національних інтересів постає інформаційний простір. Сучасні технології здатні досягти виконання власних інтересів без залучення воєнного впливу, послабити або навіть зруйнувати конкуруючу країну, не залучаючи військової сили, за умови, що ця країна не усвідомить потенційних та реальних загроз несприятливих інформаційних впливів і не зробить дієвої системи протидії і захисту цим загрозам.

РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Отже, безпека інформаційного простору є невід'ємною частиною кожної із складових забезпечення національної безпеки країни.

З урахуванням подальшого розвитку технологій передачі та отримання інформації, залученні інформаційних технологій у найголовніші сфери життя суспільства необхідно очікувати зміну від принципу забезпечення безпеки інформації до принципу інформаційної безпеки. Розглядаючи інформаційну безпеку з позиції системного підходу дозволяє відчути відмінність наукового розуміння цієї проблеми від повсякденного. У повсякденному житті інформаційна безпека вважається лише як необхідність боротьби з втратою закритої (таємної) інформації, а й також з розповсюдженням помилкової та ворожої інформацій. Розуміння нової інформаційної безпеки у суспільстві ще тільки починається.

Найважливішими складовими концепції забезпечення інформаційної безпеки є: оперативна безпека, введення супротивника в оману, психологічні операції, електронна війна, яка проводиться в комплексі з глибокою і всебічною розвідкою як для дезорганізації системи управління противника, так і для захисту власної системи управління. При цьому інформація, що циркулює в системі управління, розглядається як високопріорітетний об'єкт впливу і захисту.

Серед нових найбільш важливих засобів інформаційної обороноздатності України сьогодні називають різні математичні, програмні засоби типу «вірусів» і «закладок», засоби дистанційного витирання інформації, що записана на магнітних носіях, генераторами електромагнітних імпульсів, засоби неконтрольованого включення у закриті інформаційні мережі.

Тому на врегулювання питання інформаційної безпеки Рада національної безпеки і оборони України розробила Проект Доктрини інформаційної безпеки України, якою визначила поняття та значення інформаційної безпеки, її місце в системі забезпечення національної безпеки України, принципи та способи її реалізації. Також Проект визначає основні загрози інформаційній безпеці України, які існують як у внутрішньому так і зовнішньому просторі. Указавши загрози РНБО також зазначило і методи та способи їх подолання. Діяльність щодо забезпечення інформаційної безпеки країни є, за Конституцією України, однією з найважливіших функцій держави, справою всього українського народу. Тому основними напрямками цієї діяльності мають бути:

1. Створення законодавчої та нормативної баз;
2. Визначення компетенції органів державної влади та управління;
3. Здійснення контролю за діяльністю юридичних та фізичних осіб у сфері забезпечення інформаційної безпеки України;
4. Фінансова, наукова та матеріально-технічна підтримка юридичних та фізичних осіб, що беруть участь у створенні системи забезпечення інформаційної безпеки України;
5. Стандартизація, сертифікація та ліцензування діяльності;
6. Удосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної національної безпеки України;
7. Розробка міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки України.

ВИСНОВОК

Підводячи підсумок, необхідно зазначити, що для ефективного забезпечення інформаційної безпеки в України буде не достатньо прийняття лише нормативно-правових актів у цій сфері. Враховуючи досвід зарубіжних країн (зокрема США), доцільним буде створення при Міністерстві оборони або у складі Служби безпеки України спеціального департаменту забезпечення інформаційної безпеки та оборони, основною функцією якого є створення необхідних умов та матеріальних засобів захисту інформації, яка має гриф секретності або ж становить значну цінність для суверенного, незалежного функціонування України як самостійно держави.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Національна безпека України. Реферат» // Военное дело, ДПЮ, 30 вересня 2011 р. // http://ru.osvita.ua/vnz/reports/dpju/24540

2. «Проект Доктрини національної безпеки України (РНБО України)» // РНБО України, 25 травня 2009 р. // http://www.strateger.net/Doktrina_nacionalnoj_bezopasnosti_Ukraini

3. «Основні пріоритети інформаційної безпеки» // Національна безпека України // http://old.niss.gov.ua/book/otch/roz22

4. «Інформаційна безпека України в системі забезпечення національної безпеки» // Національний університет ДПС України, Безвершенко О. О. // http://www.rusnauka.com/13_NPN_2010/Pravo/66151.doc.htm

УДК 343.721: 004.056

РОЛЬ ИТ В ПРОЦЕССЕ ВЫЯВЛЕНИЯ И ПРЕДОТВРАЩЕНИЯ КОРПОРАТИВНОГО МОШЕННИЧЕСТВА

Пицык В. В.[1], Линевич В. Э. [2], Пархоменко А. В. [3], Мосин Е. Е. [4], Дегтярьов А. В. [5]
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: Holy_Inquisition@bigmir.net

В данной статье поднимается вопрос корпоративного мошенничества как неотъемлемого явления отечественного бизнеса. Соответственно, представлены пути предотвращения мошенничества на предприятии, а также особая роль ИТ в этом процессе.

Ключевые слова: мошенничество, безопасность, аудит, ИТ- контроль.

ВСТУПЛЕНИЕ

Урон, наносимый корпоративными преступлениями компаниям любого размера, отрасли, формы собственности, весьма существенный и проявляется не только в прямом ущербе, который относительно легко посчитать в денежном эквиваленте. Зачастую его можно представить в утраченных активах, неполученной (недополученной) прибыли, негативных репутационных последствиях и в ухудшении морального климата в трудовом коллективе [1].

Таким образом, любой факт корпоративного мошенничества наносит компании вред, который сказывается на всех основных сферах деятельности организации и зачастую имеет отложенные во времени негативные последствия, масштаб которых не всегда можно предусмотреть.

ИЗУЧЕНИЕ ПРОБЛЕМЫ

Последний раз комплексное исследование по вопросам борьбы с мошенничеством в европейских странах (в т.ч. Украины) проводилось компанией «Эрнст энд Янг» (Ernst & Young) в 2009 году. Результаты исследования свидетельствовали о наличии вызывающей разочарование толерантности сотрудников компаний по отношению к неэтичному поведению. Денежные выплаты для получения контрактов и даже намеренное искажение результатов финансовой отчетности для сокрытия результатов деятельности оправданны с точки зрения очень большого числа респондентов, что является тревожным сигналом. И со временем проблема имеет тенденцию лишь усугубляться [2].

Основополагающими для украинских компаний факторами, способствующими росту экономической преступности, являются повсеместная коррупция, угроза увольнения в период кризиса и толерантность персонала по отношению к проявлениям корпоративного мошенничества. Очень показателен факт того, что мошенничество проявляется на всех уровнях корпоративной цепочки – от низших должностей вплоть до высшего руководства. Взяточничество и хищение имущества являются наиболее распространенными экономическими преступлениями. К числу прочих относятся незаконное заимствование, манипуляции с финансовой отчетностью, налоговое мошенничество и другие.

В основе мошеннических действий персонала лежит несовершенство отдельных законов и нормативно-правовых документов, сложность и многоступенчатость финансово-экономических связей, некомпетентность и юридическая неосведомленность, беспечность и чрезмерная доверчивость руководителей, а также бесконтрольность сотрудников – [3].

Несмотря на очевидные угрозы ведению бизнеса, на практике далеко не все руководители компаний обращают внимание на факты корпоративного мошенничества в принципе, а те, что обращают, или закрывают на это глаза, либо ограничиваются увольнением виновных в случае выявления [4].

Меры пресечения мошенничества во всех странах довольно схожи, Украина — не исключение. Корпоративный сектор предпочитает проводить внутренний контроль и аудит. Достаточно распространены проверки со стороны руководства, а также внешний аудит деятельности компаний.

В компании «Эрлан» (ТМ «Биола») для противодействия фактам мошенничества тщательно подбирают персонал компании. «Мы стараемся мошенничество предупреждать еще на стадии подбора кадров. Мы интересуемся не только послужным списком, но и запрашиваем отзывы о

сотруднике на предыдущих местах работы», – PR-директор компании Анна Юнге [5].

В компании «Сандора» существует четкий перечень действий, которые считаются корпоративным мошенничеством. «Политика детально описывает, какие действия относятся к мошенничеству, и какая административная или даже уголовная ответственность применяется к нарушителям. Введена система внутреннего аудита, проверяющая ее знание и понимание», – Елена Стоянова, директор по маркетингу компании «Сандора» [6].

МЕТОДИКА РЕШЕНИЯ ПРОБЛЕМЫ

В целом, программа по управлению рисками мошенничества проводится по трем линиям обороны.

1 Кодекс корпоративной этики и политики, связанные с ним.

2 Система внутреннего контроля.

3 Деятельность служб внутреннего аудита.

К первой линии обороны можно отнести:

На основании оценки возможных рисков в компании должен быть разработан и доведен до сотрудников Кодекс Корпоративной Этики (ККЭ). Важна регулярная проверка знаний сотрудников в отношении ККЭ.

1 Наличие в компании людей, не понимающих и потому не соблюдающих существующие политики информационной безопасности, может свести на нет все усилия и затраты на защиту информации

2 Необходимо внедрение программы повышения осведомленности в области информационной безопасности и проведения соответствующих тренингов для сотрудников компании

Ко второй линии обороны можно отнести:

Эффективная система внутреннего контроля (СВК) обладает и предотвращающими, и выявляющими элементами, но не упреждающими. Она направлена в основном на подавление факторов группы «Возможность».

Общий ИТ контроль:

1 Внедрение DLP – систем.

2 Контроль разграничения прав доступа.

3 Логирование всех операций.

4 Контроль, обеспечивающий конфиденциальность ключевой информации, операций.

5 Должен быть поставлен процесс управления инцидентами, связанными с процессом управления доступом.

6 Контроль уровня приложения.

К третьей линии обороны можно отнести:

Служба внутреннего аудита во многих компаниях отвечает за выявление мошенничества, представляя третью линию обороны.

На основании оценки рисков, Служба внутреннего аудита должна выявить, критически оценить и протестировать эффективность «защитных мер» первой и второй линий обороны.

В сущности, именно Служба внутреннего аудита (или ее аналог) отвечает за выявление мошеннических действий. Расследование мошенничества может проводиться совместно с другими подразделениями (например, Службой безопасности).

1 Анализ рисков.

2 Поиск индикаторов мошенничества.

3 Сопоставление данных из различных баз данных и информационных систем.

4 Определение влияния мошенничества.

5 Проактивное тестирование.

6 Непрерывный мониторинг.

Проведение расследования: общие моменты

Система управления рисками мошенничества сфокусирована на организации в целом, а не на конкретных инцидентах. В таких случаях, основной фокус надо делать на расследованиях. Расследования становятся неотъемлемой частью системы.

В случае возникновения и выявления инцидента необходимо организовать расследование, провести его. составить отчет о результатах и довести их до руководства.

Необходимо учесть, что потенциальный конфликт интересов внутри компании может помешать проведению расследования только внутренними силами, поэтому целесообразно рассмотреть участие внешних ресурсов. Кроме того, отсутствие четкого понимания юридических последствий расследования и его результатов может существенно снизить возможности их дальнейшего использования. Поэтому целесообразно консультироваться с юристами (внешними и внутренними) на всех этапах подготовки и проведения расследования.

Рекомендуется разработать, утвердить и применять на практике внутренний документ, устанавливающий правила проведения расследования и использования его результатов – [7].

ВЫВОДЫ

В заключение следует отметить, что наиболее действенным способом борьбы с корпоративными преступлениями является сочетание профилактических мер и мероприятий по выявлению, расследованию и предотвращению последствий фактов мошенничества. Несмотря на то, что внедрение и постоянное поддержание таких систем противодействия требуют значительных ресурсных затрат, они дают существенный эффект для бизнеса компании в будущем. Введение принципа нулевой толерантности, который предполагает ужесточение санкций в отношении лиц, замешанных в мошеннических или коррупционных действиях, а также в подкупе должностных лиц, остается приоритетной задачей.

СПИСОК ИСТОЧНИКОВ

1. Говард Р. Давиа, Мошенничество: методики обнаружения, 2005г.- 200с.

2. Джозеф Т. Уэллс, Справочник по предупреждению и выявлению корпоративного мошенничества, 2008 г. – 484с.

3. Материалы выступления с круглого стола “Корпоративное мошенничество в украинских компаниях: смириться или побороться?” (Электронный ресурс) / Способ доступа: URL: http://www.slideshare.net/VolodymyrMatviychuk/ey-fraud-round-table - Роль ИТ в выявлении и предотвращении мошенничества на предприятии.

4. Материалы европейского исследования «Ernst & Young» по вопросам управления рисками мошенничества, результаты для Украины (Электронный ресурс) / Способ доступа: URL: http://www.slideshare.net/dn131282nvj/ey-ukraine-fraud-survey-may-09-rus?from=ss_embed

5. Новостная статья «Уровень корпоративного мошенничества в Украине» (Электронный ресурс) / Способ доступа: URL: http://vkurse.ua/business/uroven-korporativnogo-moshennichestva.html

УДК 681.188

ПРОБЛЕМИ КРИПТОЗАХИСТУ ШИФРУВАЛЬНОЇ МАШИНКИ «ЕНІГМА»

Бабяк Євгенія Олексіївна, Масальська Олена Олександрівна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: burnbeforeyou@yahoo.com

Шифрувальні пристрої дозволяють захистити інформацію, передану по радіоканалу, від перегляду сторонніми особами, і насамперед, спецслужбою супротивника. У загальному випадку букви і цифри повідомлення замінюються іншими символами, роблячи його абсолютно незрозумілим. Найпростіші шифри, що застосовувалися протягом століть, використовували схему прямого заміщення однієї букви інший, причому щоразу однієї і тієї ж.

Ключові слова – криптозахист; надійність шифру; безпека конфіденційної інформації .

ВСТУП

Нові способи шифрування представлялися настільки надійними, що, здавалося, противнику не вдасться їх розгадати. Тим не менш, багато з застосовувалися тоді шифрів були розкриті вже під час другої світової війни завдяки таланту вчених-криптографов і застосуванню електронно-обчислювальних машин.

«Опинитися в потрібному місці в потрібний час» - саме цим девізом я можна охарактеризувати успішність криптомашини Енігма, яку німецьке командування вважало одним з найнадійніших шифрувальних пристроїв. У 1917 році голландець Кох запатентував електричний роторний шифрувальний пристрій для захисту комерційної інформації. У 1918 році німець Шербіус купив цей патент, доопрацював його і побудував шифрувальну машину Енігма (від грец. Αινιγμα - «загадка»). Сам пристрій працював на поліалфавітному шифрі підстановки. Простою версією поліалфавітних шифрів є шифр Віженера [3]. Для свого часу це був досить просунутий метод, адже не знаючи ключового слова, його дуже важко було зламати. Чотирьохроторну машину можна було налаштувати на будь-який спосіб кодування, а способів таких було - $2 \cdot 10^{145}$. І кожен по-різному шифрував текст [1].

ОСНОВНИЙ ПРИНЦИП РОБОТИ

Ротори - серце Енігми. Кожен ротор представляв собою диск приблизно 10 см в діаметрі, зроблений з ебоніту або бакеліта, з пружинними штирьовими контактами на одній стороні ротора, розташованими по окружності. На іншій стороні знаходилося відповідну кількість плоских електричних контактів. Штирові і плоскі контакти відповідали буквах в алфавіті (зазвичай це були 26 букв від A до Z). При зіткненні контакти сусідніх роторів замикали електричний ланцюг. Всередині ротора кожен штирьовий контакт був з'єднаний з одним із плоских. Порядок з'єднання міг бути різним. При використанні декількох роторів у зв'язці (зазвичай трьох або чотирьох) за рахунок їх постійного руху виходив більш надійний шифр [1].

ОСОБЛИВОСТІ ТА ПЕРЕВАГИ ПРИСТРОЮ

«Енігма» була розроблена таким чином, щоб безпека зберігалася навіть у тих випадках, коли шпигунові відомі роторні схеми, хоча на практиці налаштування зберігаються в секреті. Більшість ключів зберігалися лише певний період часу, зазвичай добу. Однак для кожного нового повідомлення задавалися нові початкові позиції роторів. Це обумовлювалося тим, що якщо число повідомлень, посланих з ідентичними налаштуваннями, буде велике, то криптоаналитик, який досконало вивчив стільки повідомлень, може підібрати ключ до повідомлень, використовуючи частотний аналіз. Для надійності шифру так само часто вживані слова та імена дуже сильно варіювалися. Наприклад, слово «Minensuchboot» могло бути написано як «MINENSUCHBOOT», «MINBOOT», «MMMBOOT» або «MMM354». Щоб ускладнити криптоаналіз, окремі повідомлення не містили понад 250 символів. Довші повідомлення розбивалися на частини, кожна з яких використовувала свій ключ.

СИСТЕМИ ЗНЕШКОДЖЕННЯ «ЗАГАДКИ» ПІД КОДОВОЮ НАЗВОЮ «ULTRA»

Злом англійцями німецьких шифрувальних машин, тобто машинне розгадування способу шифрування текстів в них, отримала англійську назву ULTRA. Немашинні методи дешифрування були занадто трудомісткими і в умовах війни неприйнятними. Для цієї роботи англійці об'єднали приблизно 10 000 осіб, у тому числі математиків, інженерів, лінгвістів, перекладачів, військових експертів, а також інших співробітників для сортування даних, їх перевірки та архівування, для обслуговування машин. Це об'єднання носило назву BP (Bletchley Park - Блетчлі парк), воно знаходилось під контролем особисто Черчілля. Отримана

інформація виявилася в руках союзників могутньою зброєю. Англійські військові і особисто Черчиль вимагали постійної уваги до розшифровки повідомлень. Починаючи з літа 1940р. англійці розшифровували всі повідомлення, зашифровані за допомогою Енігми. Тим не менш, англійські фахівці безперервно займалися вдосконаленням дешифровальной техніки. До кінця війни англійські дешифратори мали на своєму озброєнні 211 цілодобово працюючих дешифрирувальних пристроїв. Їх обслуговували 265 механіків, а для чергування були залучені 1675 жінок. Роботу творців цих машин оцінили через багато років, коли спробували відтворити одну з них: через відсутність на той момент необхідних кадрів, робота з відтворення відомого пристрою тривала кілька років і залишилася незакінченою!

Створена тоді Т'юрінгом інструкція по створенню дешифрируются пристроїв перебувала під забороною до 1996 року. Серед засобів дешифрування був метод «примусовою» інформації: наприклад, англійські літаки руйнували пристань у порту Калле, свідомо знаючи, що далі слідуватиме повідомлення німецьких служб про це з набором заздалегідь відомих англійцям слів! Крім того, німецькі служби передавали це повідомлення багато разів, щоразу кодуючи його різними шифрами, але слово в слово.

Нарешті, найважливішим фронтом для Англії була підводна війна, де німці використовували нову модифікацію ЕнігмаМ3. Англійський флот зміг вилучити таку машину з захопленого ними німецького підводного човна. З 1 лютого 1942 ВМФ Німеччини перейшов на користування моделлю М4. Але деякі німецькі повідомлення, зашифровані по-старому, помилково містили інформацію про особливості конструкції цієї нової машини. Це сильно полегшило завдання команді Т'юрінга. Уже в грудні 1942р. була зламана Енігма М4. 13 грудня 1942 англійське Адміралтейство отримало точні дані про місцезнаходження 12 німецьких підводних човнів в Атлантиці.

На думку Т'юрінга, для прискорення дешифрування необхідно було переходити до використання електроніки. 7 листопада 1942 Тюрінг відправився в США, де разом з командою з лабораторій Белла були вдосконалені американські дешифрувальні машини, так що Енігма М4 була зламана остаточно і до кінця війни давала англійцям і американцям вичерпну розвідувальну інформацію. Тільки в листопаді 1944 року у німецького командування виникли сумніви в надійності своєї шифрувальної техніки, проте ні до яких заходів це не призвело [4].

ВИСНОВКИ

Енігма представляла собою досить зручну шифрувальну машину: одержуваний шифр був досить складний, а сама процедура кодування розкодування була досить проста. Також невід'ємним перевагою шифру Енігми є висока швидкість кодування розкодування. Крім того, процедура кодування дуже проста з вигляду і наочна.

З появою комп'ютерів надійність такого шифру впала, тому код має досить багато важливих особливостей, що спрощують злом, тому в сучасних системах таке шифрування застосовують досить рідко.

СПИСОК ВИКОРИСТАННОЇ ЛИТЕРАТУРИ

1. Жельников В. Криптографія від папірусу до комп'ютера. М .: ABF, 1996. 336 с.
2. Смарт Н. Криптографія. Серія «Світ програмування». Пров. з англ. С. А. Кулешова / Под ред. С. К. Ландо. М .: Техносфера, 2005. 528 с.
3. Шнайер Б. Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Сі. М .: Тріумф, 2003. 816 с.
4. Таємниця проекту Ultra // OSP.ru, 2003-07-08 Режим доступу: http://www.osp.ru/os/2003/07-08/183294/

УДК 004.415.5

ОСОБЕННОСТИ СЕРТИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Лебедь Оксана Олеговна, Масальская Елена Александровна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: Ksy4308@yandex.ru

Во всем мире сегодня практикуется тестирование кода информационных систем по требованиям безопасности информации, однако, несмотря на расширение практики сертификации, вокруг него сложился ряд заблуждений.

Ключевые слова – система сертификации; безопасность конфиденциальной информации.

ВВЕДЕНИЕ

В нашей стране традиционно преобладают директивные методы оценки соответствия, а программное обеспечение ряда информационных систем подлежит обязательной сертификации по требованиям безопасности информации.

Исторически система сертификации по требованиям безопасности информации в Украине возникла после распада СССР, когда появилась потребность в контроле безопасности зарубежного программного обеспечения, а также качества украинских программных систем, связанных с обработкой и защитой государственной тайны.

ОСНОВНЫЕ ЦЕЛИ СЕРТИФИКАЦИИ

До недавнего времени сертификация главным образом касалась силовых министерств и предприятий промышленности, выполняющих

государственные заказы, а основная масса специалистов в области информационных технологий мало интересовалась данной проблемой.

Оказывается, что сертификация программного обеспечения и аттестация объектов информатизации необходима большинству коммерческих компаний и всем государственным организациям, работающим в области медицины, образования, транспорта. В связи с этим возникло множество вопросов и, как правило, негативных суждений, связанных в большинстве случаев с недопониманием сути и процессов сертификации.

В общем случае под сертификацией принято понимать независимое подтверждение соответствия тех или иных характеристик товаров или услуг некоторым требованиям. В нашем случае речь идет о программных средствах защиты или программ в защищенном исполнении – соответственно в качестве требований выступают нормативные документы и документация, касающаяся безопасности информации [1].

ОСОБЕННОСТИ ПРОВЕДЕНИЯ СЕРТИФИКАЦИИ

Принципиальная особенность любых сертификационных испытаний – это независимость испытательной лаборатории, проводящей испытания, и сертифицирующей организации, осуществляющей независимый контроль результатов испытаний, проведенных лабораторией. В общем случае схема проведения сертификации выглядит следующим образом.

1. Заявитель (разработчик либо другая компания, заинтересованная в проведении сертификации) подает в государсвенную службу специальной связи по сертификации заявку на проведение сертификационных испытаний некоторого продукта.
2. Государственный орган определяет аккредитованную испытательную лабораторию и орган по сертификации.
3. Испытательная лаборатория совместно с заявителем проводит сертификационные испытания. Если в процессе испытаний выявляются те или иные несоответствия заявленным требованиям, то они могут быть устранены заявителем в рабочем порядке, что и происходит в большинстве случаев, либо может быть принято решение об изменении требований к продукту, например, о снижении класса защищенности.
4. Материалы испытаний передаются в орган по сертификации, который проводит их независимую экспертизу. Как правило, в экспертизе участвуют не менее двух экспертов, которые независимо друг от друга подтверждают корректность и полноту проведения испытаний.
5. Государственный орган по сертификации на основании заключения органа по сертификации оформляет сертификат соответствия. Надо сказать, что в случае выявления каких-либо несоответствий государственный орган может провести дополнительную экспертизу с привлечением экспертов из различных аккредитованных лабораторий и органов.

В системах обязательной сертификации имеется практика отзыва и приостановления лицензий и аттестатов аккредитаций в случае выявления грубых нарушений в процессе сертификации [2].

СИСТЕМЫ СЕРТИФИКАЦИИ И ТРЕБОВАНИЯ К НИМ

Сертификация средств защиты информации может быть добровольной или обязательной. Добровольные системы сертификации средств защиты информации на сегодняшний день пока еще не получили широкого распространения. К сожалению, несмотря на то, что в добровольных системах можно получить сертификат на соответствие любому нормативному документу по защите конфиденциальной информации, при аттестации объектов информатизации такие сертификаты не признаются.

Что касается документов, на соответствие которым проводятся сертификационные испытания, то они практически идентичны во всех системах сертификации. Существуют два основных подхода к сертификации – и соответственно два типа нормативных документов.

1. Функциональное тестирование средств защиты информации, позволяющее убедиться в том, что продукт действительно реализует заявленные функции. Это тестирование чаще всего проводится на соответствие конкретному нормативному документу. Такие документы установлены, например, для межсетевых экранов и средств защиты от несанкционированного доступа. Если же не существует документа, которому сертифицируемый продукт соответствовал бы в полной мере, то функциональные требования могут быть сформулированы в явном виде – например, в технических условиях, или в виде задания по безопасности.
2. Структурное тестирование программного кода на отсутствие недекларированных возможностей. Классическим примером недекларированных возможностей являются программные закладки, которые при возникновении определенных условий инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию. Выявление недекларированных возможностей предполагает проведение серии тестов исходных текстов программ, предоставление которых является необходимым условием для возможности проведения сертификационных испытаний.

В большинстве случаев средство защиты информации должно быть сертифицировано как в части основного функционала, так и на предмет отсутствия недекларированных возможностей. Делается исключение для систем обработки персональных данных второго и третьего класса с целью снижения затрат на защиту информации для небольших частных организаций. Если программное средство не имеет каких-либо механизмов защиты информации, оно может быть сертифицировано только на предмет отсутствия недекларированных возможностей [3].

ВЫВОДЫ

Сертификация не является универсальным способом решения всех существующих проблем в области информационной безопасности, однако сегодня это единственный реально функционирующий механизм, который обеспечивает независимый контроль качества средств защиты информации, и пользы от него больше, чем вреда. При грамотном применении механизм сертификации позволяет вполне успешно решать задачу достижения гарантированного уровня защищенности автоматизированных систем.

Заглядывая вперед, можно предположить, что сертификация как инструмент регулятора будет изменяться в направлении совершенствования нормативных документов, отражающих разумные требования по защите от актуальных угроз, с одной стороны, и в направлении улучшения методов проверки критических компонентов по критерию «эффективность/время» – с другой.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Т. 2: Информационная безопасность. – К.: Арий, 2008, – 344 с.
2. Методы информационной защиты объектов и компьютерных сетей / А.В. Соколов, О.М. Степанюк. СПб.: ООО “Издательство Полигон”, 2000.
3. МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 27001 Первое издание 2005-10-15 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования

УДК 004.056.53

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ HEARTBLEED АТАКИ НА HEARTBEAT В OPENSSL

Сизинцев Н.А.

Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина, http://bit.nmu.org.ua, E-mail: nas8717@gmail.com

В работе рассматривается критическая уязвимость в Heartbeet функционале в криптографическом пакете OpenSSL. Приведен результат атаки на данную уязвимость.

Ключевые слова: HeartBleed, OpenSLL, HeartBeet.

ВВЕДЕНИЕ

OpenSSL – криптографический пакет с открытым исходным кодом для работы с SSL/TLS. Позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать CSR и CRT. Также имеется возможность шифрования данных и тестирования SSL/TLS соединений[1]. Данный криптографический пакет широко используется для обеспечения HTTPS соединения на сайтах, банковских шлюзах и т.д.

В марте 2014 года специалисты из финской компании Codenomicon и сотрудник Google Neel Mehta обнаружили критическую уязвимость в реализации функции Heartbeat, в переводе "Сердцебиение". Данная функция отвечает за проверку соединения между клиентом и сервером, она реализована путем обмена короткими периодическими сообщениями между ними.

1 января 2012 года, Robin Seggelmann отправил, а steve проверил commit[2] на GitHub, который добавлял HeartBeat в OpenSSL. Именно этот commit внес критическую ошибку, позднее названную Heartbleed.

HEARTBLEED В OPENSSL

По идее, запрос и ответ должны были быть одинаковой длины, но из-за уязвимости, одна сторона могла послать запрос длиной в пару десятков байт, а запросить ответ длинной до 64КБайт, который выбирался из памяти. В этом кусочке памяти мог быть и мусор, равно как и данные пользователей или иные полезные данные, например, ключ шифрования другой стороны.

Код в OpenSSL, который приводит к ошибке:

```
int
dtls_process_heartbeat (SSL *s)
{
unsigned char *p=&s->s3->rrec.data[0], pl*;
unsigned short hbtype;
unsigned int payload;
unsigned int padding = 16;
```

Данный метод отвечает за обработку Heartbeat запроса. В первой строке мы получаем указатель на данные в записи SSLv3.

```
typedef struct ss13_record_st
{
int type;
unsigned int off;
unsigned char *data;
unsigned char *input;
unsigned char *comp;
unsigned long epoch;
unsigned char seq_num[8];
} SSL3_RECORD;
```

Запись SSLv3 представляет из себя структуру, которая содержит тип Heartbeat запроса, длину входящих данных и данные, необходимые для работы.

```
hbtype = *p++;
n2s (p, payload);
pl = p;
```

Первый байт в SSL записи - тип "сердцебиения", он записывается в переменную hbtype, макрос n2s записывает два байта из в payload, данная переменная определяет длину полезных данных.

Затем pl получает данные "сердцебиения", предоставленные запрашивающим. Далее следует код:

```
unsigned char *buffer, *bp;
int r;
buffer = OPENSSL_malloc(1 + 2 + payload +
padding);
bp = buffer;
```

В указатель buffer выделяется столько памяти, сколько запросила вторая сторона: до 1 + 2 + 65535 + 16.

```
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp) ;
memcpy(bp, pl, payload);
```

Функция memcpy копирует количество байт равных payload, начиная с адреса pl в адреса начиная с адреса в bp.

Уязвимость заключается в том, что сторона, обрабатывающая запрос, не проверяет фактическую длину данных, а выделяет и копирует памяти столько, сколько отправила запрашивающая сторона. Так как запрашивающая сторона в действительности может не передать количество байт, которое она указала, то выделенная память не будет перезаписана, а назад отправятся данные которые там находились.

Использование данной уязвимости реализовано в множестве эксплойтов[3], один из них доступен по ссылке[4]. Он написан на Python и позволяет производить указанное кол-во heartbeat запросов на сервер по указанному адресу.

В статье "Чем грозит Heartbleed простому пользователю?"[5], автор привел результат использования уязвимости heartbleed на банковском шлюзе:

"В нем было все. Буквально все, что проходит через платежный шлюз: номер заказа, номер карты, CVV2, ФИО, год и месяц до которого она действительна. За полчаса работы скрипта в дампе оказалось несколько сотен реальных банковских карт и данных об их владельцах."

Данной уязвимости были подвержены 27% HTTPS и 11% TLS ресурсов, входящих в Alexa Top 1 Million [6].

Для проверки ресурсов на уязвимости в OpenSSL существует множество ресурсов, один из них доступен по ссылке[7].

ВЫВОД

На данный момент эта угроза перестала быть критичной, так как вышел пакет обновлений, исправляющий эту уязвимость. Однако, по неизвестным причинам некоторые ресурсы по-прежнему не воспользовались этим обновлением или не отказались от использования Heartbeet.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. OpenSSL - Википедия(Электрон. ресурс) / Способ доступа: URL: https://ru.wikipedia.org/wiki/OpenSSL. – Загол. с экрана

2. PR:2658 bd6941c openssl/openssl(Электрон. ресурс)/ Способ доступа: URL: https://github.com/openssl/openssl/commit/bd6941cfaa31ee8a3f8661cb98227a5cbcc0f9f3#diff-38dc72994741420e2b6c5ee074941a45. - Загол. с экрана.

3. Эксплойт - Википедия(Электрон. ресурс)/ Способ доступа: URL: https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82/. – Загол. с экрана.

4. Heartbleed (CVE-2014-0160) Test & Exploit Python Script(Электрон. ресурс)/ Способ доступа: URL: https://gist.github.com/eelsivart/10174134. – Загол. с экрана.

5. Чем грозит Heartbleed простому пользователю? (Электрон. ресурс)/ Способ доступа: URL: http://habrahabr.ru/post/219151/. – Загол. с экрана.

6. Alexa Top 1m Global Sites(Электрон. ресурс) / Способ доступа: URL: http://s3.amazonaws.com/alexa-static/top-1m.csv.zip. – Загол. с экрана.

7. Qualys SSL Labs(Электрон. ресурс) / Способ доступа: URL: https://www.ssllabs.com/. – Загол. с экрана.

УДК 35.078.3

МАНІПУЛЯЦІЇ ГРОМАДСЬКОЮ ДУМКОЮ ЗА ДОПОМОГОЮ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Легенченко Катерина Олегівна

Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна, http://bit.nmu.org.ua, E-mail: Katleg@mail.ru

У тезі висвітлюються методи та можливі наслідки маніпулювання свідомістю громадян завдяки засобам масової інформації.

Ключові слова – засоби масової інформації; суспільна свідомість; національна безпека.

ВСТУП

Інформація займає важливе місце у розвитку сучасного суспільства. Вона стає одним з актуальних джерел для розвитку, до того ж завдяки мережі Інтернет її стає все більше. Швидке виробництво інформації активно впливає на інформатизацію суспільства в цілому. У всьому світі циркулює величезна кількість інформаційних потоків, формуючи тим самим громадські думку й погляд на різні речі. Контролюючи ці інформаційні потоки, певні групи людей можуть не тільки аналізувати суспільні настрої, обмежувати кількість інформації, представляти певні події з вигідної їм точки зору, а й змінити історію і її подальший розвиток, повернувши погляди людей у певному напрямку. Це явище дуже гостро зачіпає тему національної безпеки в цілому.

ДОСЛІДЖЕННЯ

Згідно Закону України «Про основи національної безпеки України», національна безпека - захищеність

життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам.[1]

Варто взяти до уваги, що подальший розвиток країни можна змінити шляхом нав'язування хибної інформації. Тому однією з найважливіших функцій служб національної безпеки різних країн є контроль інформаційних потоків, що формують хвилювання в суспільстві.

Формування суспільної свідомості шляхом нав'язування конкретної інформації - далеко не сучасне нововведення. Приклади маніпулювання великими масами людей для певної вигоди відомі в різні часи.

Під час Другої світової війни необхідність мобілізувати збройні сили і населення для ведення важкої війни, а також впливати на ворожу армію і населення зайнятих ворожих територій обернулася розквітом у країнах, що воюють, різних пропагандистських технологій, які стали невід'ємною частиною самої війни. Використовувалися не тільки плакати й різноманітні листівки, але і звукозаписи, радіопрограми, прямі пропагандистські аудіотрансляції на ворожі окопи, створення колабораціоністських організацій.

Рівень обробки цільових груп виявлявся дуже високим. Наприклад, значна частина населення Німеччини ще на початку весни 1945 була впевнена у неминучій перемозі, тоді як насправді результат війни вже був визначений. Природно, що ці дії відбувалися для підтримки бойового духу населення.

Соціальні мережі та засоби масової інформації були також міцною платформою для хвилі демонстрацій і путчів в арабському світі, іменованої як Арабська весна. Перевороти в Тунісі, Єгипті та Ємені, громадянські повстання в Бахрейні і масові протести в Алжирі, Іраку, Йорданії, Марокко та Омані були організовані за допомогою поширення інформації про ідеї переворотів і повстань, місця і обставини демонстрацій через соціальні мережі та засоби масової інформації (ЗМІ). Внаслідок цього влада Тунісу, Єгипту та Лівії змушені були провести відключення сучасних засобів комунікації: зупинили надання послуги доступу до мережі Інтернет великими провайдерами, частково відключили мобільний зв'язок, блокували сторінки у соціальних мережах і видаляли провокаційні повідомлення.

Недарма династія Ротшильдів, європейських банкірів і громадських діячів, ще в дев'ятнадцятому сторіччі стверджувала: «Хто володіє інформацією - той володіє світом».

Існує два основних джерела формування й розвитку громадської думки. По-перше, це безпосереднє спостереження за навколишнім середовищем, схвалення або осуд тих чи інших дій, рішень й висловлювань. По-друге, це засоби масової інформації, які надають цілеспрямований вплив на думки, оцінки та поведінку людей.

У соціумі інформаційні впливи спрямовані на формування масової та індивідуальної свідомості. Вони досягають ефекту, коли змінюють психологічні властивості і моделі поведінки та діяльності особистості й суспільства в потрібному напрямку.

Інформаційно-психологічні дії можуть впливати на всі компоненти свідомості: психічні процеси (пам'ять, уяву, мислення, увагу), психологічні стани та психічні властивості особистості.

Застосування засобів інформаційно-психологічного впливу на людину може призвести до зміни психіки і психологічного здоров'я або зрушень у цінностях, життєвих позиціях, орієнтирах, світогляді індивіда, тобто в тому, що визначає особистість як громадянина.

Вплив на психіку людини може носити як конструктивний, так і деструктивний характер. У сфері соціального управління для досягнення політичних та інших цілей жорстко сплітаються конструктивні і деструктивні засоби оволодіння психікою людини шляхом маніпулювання її свідомістю.

Наявність різноманітних технічних засобів, сучасних технологій та засобів масової інформації призвело до того, що інформаційно-психологічний вплив можна спрямовувати не тільки на окрему людину, а й на велику групу людей (у тому числі на жителів окремих регіонів, країн, на суспільства в цілому).

Можна виділити три рівні об'єктів, на які спрямовано інформаційно-психологічний вплив:

- людина як громадянин - суб'єкт суспільно-політичного життя (носій світогляду, володар правосвідомості та менталітету, духовних ідеалів і ціннісних настанов). Ключовим фактором тут є довіра до влади. Формування цієї довіри - це основна політична задача соціального управління, що прямо або побічно використовує всі наявні в його розпорядженні засоби інформаційного впливу на громадян, насамперед державні ЗМІ;
- людина як особистість - індивід, що володіє свідомістю, схильною до інформаційних впливів, результати яких можуть прямо загрожувати фізичному або психологічному здоров'ю. Протиправне проповідництво може служити прикладом таких впливів, що приводять до соціальної та особистісної дезадаптації, а в ряді випадків до руйнування психіки людини;
- схильні до інформаційних впливів групи і маси людей, у яких можна викликати задану поведінку. Такою групою може бути населення країни в цілому або окремих її регіонів. До найбільш схильної до маніпулятивних впливів частини населення належать, насамперед, соціально незахищені громадяни, які відчувають сильний психологічний тиск фактів невлаштованості їхнього життя. ЗМІ можуть посилювати цей ефект потоком негативних інформаційних впливів, що обрушуються на голови соціально-незадоволених людей.[2]

Слід звернути увагу, що в сучасному суспільстві маніпуляції свідомістю людей за допомогою засобів масової інформації виявляються найбільш дієвими за масштабами впливу на аудиторію.

ЗМІ в тоталітарній державі маніпулюють громадською думкою, що досягається особливим

піднесенням, замовчуванням та приховуванням інформації.

Завдання ЗМІ для демократичного суспільства принципово інше: дати інформацію для самостійного судження людей. Це сприяє зростанню духовності в суспільстві, спонукає до активної громадської діяльності, полегшує самореалізацію особистості і стабілізує суспільне життя взагалі. ЗМІ відіграють основну роль серед засобів інформаційно-психологічного впливу.

Виділимо найпоширеніші й дієві методи маніпулювання масами за допомогою ЗМІ.[3] Причому слід звернути увагу на те, що всі ці способи успішно діють і при маніпулюванні у звичайному житті:

1. Принцип першочерговості.
2. Розповіді «очевидців» подій.
3. Активне створення образу ворога.
4. Зміщення акцентів та переорієнтація уваги.
5. Емоційне заряджання.
6. Недоступність інформації та однобічність висвітлення подій.
7. Помилкове загострення пристрастей.
8. Ефект «інформаційного штурму».
9. Схвалення удаваної більшості.
10. Маніпулятивне коментування.
11. Створення ефекту присутності.
12. Постійне повторення.

Психологічна маніпуляція - це, насамперед, тип впливу на індивіда чи якусь соціальну групу з метою змінити сприйняття та поведінку людей методом шахрайської, прихованої тактики. Відомо, що людина рідко охоче робить щось, що суперечить її бажанням і переконанням. Основне завдання маніпулювання полягає в тому, щоб завуальовано переконати людей в необхідності певних дій і непомітно нав'язати їм думку, яка допоможе маніпулятору в його подальшій діяльності.

ВИСНОВОК

Кожній людині слід більш уважно ставитися до себе, і при потраплянні до неї будь-якої інформації включати в першу чергу розум, а не почуття, для аналізу подібної інформації. Рейхсміністр народної освіти і пропаганди Німеччини Йозеф Геббельс стверджував: «Найгірший ворог будь-якої пропаганди – інтелектуалізм». Для формування тверезого погляду на різні речі, для передумов тому, щоб людина вчилася думати і аналізувати - головне, щоб інформація завжди була якісною і достовірною. Але, на жаль, у більшості своїй, це далеко не так. Тому кращим способом об'єктивного оцінювання подій є вивчення поглядів на цю пригоду з різних джерел і формування своєї особистої неупередженої думки.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основи національної безпеки України».
2. Ларин А. В., Остапенко А. Г. Информационное управление в социальных системах. Международный институт компьютерных технологий, г. Воронеж, Россия (Электронный ресурс) / URL: http://waorks.tarefer.ru/16/100051/index.html.
3. Зелинский С. А. Манипуляции массами и психоанализ. Манипулирование в СМИ, 2005 (Электронный ресурс) / URL: http://psyfactor.org/lib/zel3.htm.

УДК 65.012.8

СЦЕНАРНИЙ АНАЛІЗ ЯК МЕТОДОЛОГІЧНА ОСНОВА КЕРУВАННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Шеліхов Сергій Вячеславович[1], Масальська Олена Олександрівна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: vvshelikhov@gmail.com[1]

У роботі висвітлюється сценарний аналіз як один з основних компонентів процесу передбачення. Розглянуто етапи сценарного аналізу та методи, що в них застосовуються.

Ключові слова – сценарний аналіз; технологічне передбачення; інформаційна безпека.

ВСТУП

На сьогоднішній день все більш актуальною стає задача відтворити майбутнє, яке не може інтерпретуватися як звичайне продовження минулого у зв'язку з тим, що це майбутнє може набувати принципово відмінні форми та структури в порівнянні з тим, що було відомо в минулому. Ця проблема отримала назву передбачення.

Слід відзначити, що універсальних і бездоганних підходів до вирішення цієї проблеми на сьогодні не існує – наявні лиш спроби побудови можливих сценаріїв розвитку тих чи інших явищ. Однак принциповою відмінністю від попередньої практики вирішення подібних задач є те, що методи, які для цього використовуються, мають не кількісний, а якісний характер [1].

Можна вважати, що передбачення – це процес прийняття рішень для складних систем з людським фактором щодо можливої їх майбутньої поведінки. Цей процес формується за допомогою універсальної методології, відомої як сценарний аналіз.

ДОСЛІДЖЕННЯ

Сценарний аналіз – це універсальна сукупність засобів і підходів, що являє собою комплекс математичних, програмних, логічних і організаційних засобів та інструментів для визначення послідовності

застосування окремих методів, взаємозв'язку між ними та формування процесу передбачення в цілому [1].

Послідовність основних етапів, що виконуються в методології сценарного аналізу в процесі технологічного передбачення зображено на рисунку 1.

На першому етапі вивчаються проблеми та об'єкт передбачення за допомогою методів якісного та кількісного аналізу, після чого здобута інформація зводиться до єдиної платформи. Після цього визначається послідовність використання окремих методів та встановлюються взаємозв'язки між ними.

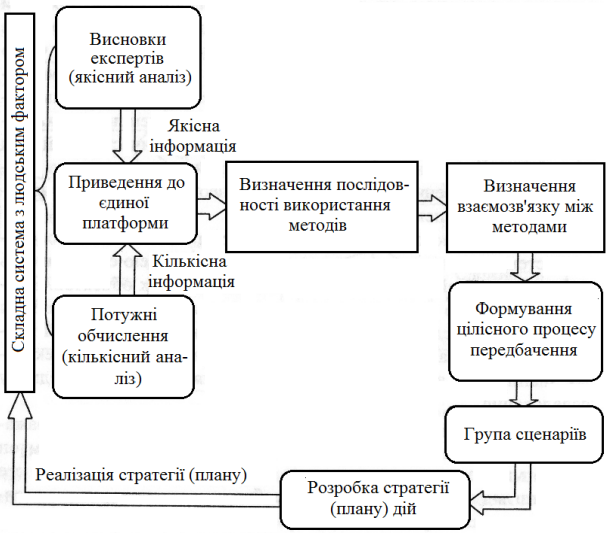


Рисунок 1. Етапи сценарного аналізу

Аналізуючи характеристики та особливості розроблених сценаріїв, група осіб, що приймають рішення (далі – ОПР), відбирає цікаві для неї сценарії, розробляє план дій відносно об'єкта передбачення та забезпечує реалізацію цього плану.

Для вирішення задач передбачення у сценарному аналізі відібрано та адаптовано 8 методів якісного аналізу. Ці методи використовуються на 4 етапах передбачення:

- 1-й етап – попереднє вивчення проблеми;
- 2-й етап – якісний аналіз проблеми;
- 3-й етап – розробка сценаріїв;
- 4-й етап – аналіз та відбір сценаріїв.

МЕТОДОЛОГІЯ СЦЕНАРНОГО АНАЛІЗУ

На першому етапі як основні застосовуються два методи: сканування та мозкового штурму.

Метод сканування полягає в наступному:

1. Створюються групи експертів.
2. Кожен експерт «генерує» ідею щодо вирішення існуючої проблеми або охарактеризувати можливі підходи до вирішення.
3. ОПР розглядають всі рекомендації експертів. Мета – «кластеризація» (тобто розподілення на групи) всіх ідей та суджень, що були виказані.
4. ОПР із усіх кластерів відбирають так звані конструктивні кластери, котрі будуть використані на наступних етапах.

Метод мозкового штурму складається з наступних кроків:

1. Сформувати проблему в заданому вузькому фокусі (вузька постановка задачі).
2. Створити групу експертів у заданій вузькій сфері знань відповідно до сформульованої проблеми.
3. В умовах обмеженого часу та переліку критеріїв експертам необхідно «згенерувати» велику кількість ідей та підходів до вирішення проблеми і відносять їх до часової перспективи дослідження.
4. «Згенеровані» судження розподілити на дві часові групи: судження, що актуальні на майбутнє (наприклад, на період не менш 5 років), та судження, що актуальні у поточний період часу і тому не використовуються.
5. Відібрати та задокументувати ідеї, котрі будуть виконуватися на подальших етапах передбачення.

Варто зауважити, що на першому етапі немає обговорень та дискусій щодо запропонованих експертами рішень, незалежно від використовуваного методу [1].

На другому етапі використовують іншу групу методів. Розглянемо один із найвідоміших – метод Делфі, або метод експертних оцінок:

1. Підбір групи експертів відповідно до проблеми, що розглядається.
2. Формулювання цілі, яку необхідно досягти при вирішенні проблеми.
3. Розробка опитувальної форми для групи експертів.
4. Опитування експертів відповідно до форми.
5. Статистична обробка даних з опитування з метою отримання загальних результатів.
6. Аналіз кожним експертом отриманих результатів.
7. В разі, якщо деякі експерти хочуть скорегувати свої відповіді, то після п.6 - повторна обробка даних згідно п.5.
8. Пункти 5-7 повторити, доки всі експерти не перестануть корегувати свої відповіді. Отриманий результат називають консенсусним.
9. Аналіз консенсусного результату з метою його чіткої інтерпретації для подальшого використання в наступних етапах передбачення.

Окрім методу Делфі широко розповсюджені також методи перехресного впливу, морфологічного аналізу та метод Сааті. Завдяки певним відмінностям у підходах до визначення результату всі ці методи загалом мають високу взаємодоповнюваність [2].

На третьому етапі використовується 9-крокова процедура побудови сценаріїв («написання сценаріїв»), яка виглядає наступним чином:

1. Визначення цілі написання сценаріїв.
2. Розроблення програми STEEPPV (інструмент аналізу оточення, що дозволяє виявляти можливості і загрози по відношенню до аналізованого об'єкту з точки зору поставленої мети).
3. Введення в сценарій припущень.
4. Побудова альтернативної схеми подій.
5. Написання сценарію.
6. Аналіз сценарію з урахуванням відгалужень і поворотних моментів.
7. Формування політики для сценарію.
8. Розроблення альтернативних стратегій поведінки суб'єктів сценарію.
9. Оцінювання альтернативних стратегій методом

імітаційного моделювання.

Нарешті, на четвертому етапі сценарії передаються особам, що приймають рішення, і проводиться загальний аналіз цих сценаріїв відповідно до наступної процедури:

- визначення рівня реалістичності та ступінь реалізованості кожного сценарію;
- оцінка ймовірності подій, що лежать в основі кожного сценарію;
- оцінка ризиків, пов'язаних з кожним сценарієм;
- імітаційне моделювання;
- вибір найбільш задовільних сценаріїв з точки зору вказаних вище критеріїв.

Визначення рівня реалістичності та ступені реалізованості кожного сценарію виконується згідно з процедурою пошуку до кожної події контр прикладу або «анти-події», яке виключає можливість здійснення події, що розглядається. Якщо таку «анти-подію» вдається знайти, то рівень довіри до сценарію з цією подією знижується [2].

ВИСНОВКИ

На сьогоднішній день технологічне передбачення стало необхідним інструментом прийняття, як мінімум, стратегічних рішень для органів управління всіх рівнів – від державних, які відповідають за розвиток країни в цілому, до управлінського персоналу окремих організацій та підприємств. Однак крім рішень, які стосуються розвитку організації, сценарний аналіз може бути використаний і для розв'язання проблем, пов'язаних із інформаційною безпекою – наприклад, у сфері керування інцидентами та при розробці контрзаходів. Це можливо тому, що методологія сценарного аналізу має в своєму складі всі необхідні засоби та інструменти для розроблення та впровадження заходів протидії загрозам інформаційній безпеці об'єкту, значно полегшуючи виконання задачі для менеджера ІБ, оскільки він на час виникнення інциденту матиме повний інструментарій для ефективної йому протидії.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Згуровський М.З., Панкратова Н.Д. Технологическое предвидение – К.: ІВЦ "Видавництво «Політехніка»", 2005. – 156 с.
2. Згуровський М.З. Геоекономічні сценарії розвитку і Україна - К. : Академія, 2010. – 323 с.

УДК 676.067.4

ЗАДАЧІ, ЩО ВИРІШУЄ ТЕХНОЛОГІЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

Карібов Руслан Азмірович[1], Мілінчук Юлія Анатоліївна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: trustmightycrusher@gmail.com[1]

В статті висвітлюється технологія цифрових водяних знаків як один із основних засобів вирішення проблеми захисту авторського права. В роботі розглянуті різноманітні сфери, в яких використовується технологія, та задачі, які вона здатна вирішити.

Ключові слова – цифровий водяний знак; ідентифікація; контент.

ВСТУП

Цифровий водяний знак – технологія, створена для захисту авторських прав мультимедійних файлів. За допомогою спеціального програмного забезпечення ЦВЗ може бути інтегрований у зображення, аудіо- чи відео файл. У більшості випадків ЦВЗ непомітний для людського ока; для його ідентифікації використовуються комп'ютери та інші цифрові прилади, після чого продукт інтелектуальної власності визнається справжнім або підробним.

Епоха розвинених цифрових технологій відкрила безліч можливостей як для авторів контенту, так і для його споживачів. За відсутності надійного засобу ідентифікації власника файл легко може бути скопійованим, зміненим, викладеним для загального використання або навіть проданим – і все це без дозволу його реального власника. Ці обставини роблять проблему використання ЦВЗ напрочуд актуальною.

БОРОТЬБА З ПІРАТСТВОМ

Піратство у сферах музики та кіно – велика проблема, що підриває розвиток індустрії розваг та наносить шкоду усім її учасникам. Сучасні формати розповсюдження вже включають в себе технології захисту, що контролюють доступ до файлів та обмежують їх несанкціоноване використання. У свою чергу, «пірати» намагаються обійти захист, щоб отримати незахищену копію, яку можна вільно розповсюджувати. Використання ЦВЗ забезпечує додатковий рівень захисту шляхом інтегрування ЦВЗ, які визначають, чи легально використовується матеріал. Обробляючий прилад считує ЦВЗ під час програвання або копіювання файлу; якщо ЦВЗ вказує на несанкціоноване використання, то дія з файлом припиняється, а замість нього відображається повідомлення, що свідчить про порушення авторських прав. Технологія ЦВЗ також допомагає власнику контенту відстежити несанкціоноване використання його власності. Для цього у момент виготовлення персональної копії або у момент її

передачі до ЦВЗ заносяться дані, що містять інформацію про час передачі, формат переданого файлу та IP-адресу отримувача. Коли з'являється підозра витоку інформації, ЦВЗ «витягується» і згодом використовується в якості доказу у факті правопорушення [1].

ЦИФРОВІ ВОДЯНІ ЗНАКИ У БІЗНЕС-СФЕРІ

У сучасному світі зображення та документи переміщуються на великі відстані з великою швидкістю великою кількістю способів. Відстежувати та захищати ці файли настільки ж складно, настільки і важливо.

Саме тому все більше компаній починає використання ЦВЗ. Наприклад, ЦВЗ може бути легко інтегрований у будь-який конфіденційний документ. Завдяки цьому можливо відстежити не тільки отримувача файлу, але і отримувати повідомлення про випадки завантаження файлу для загального використання або пересилку шляхом електронного листування за межі компанії. Декодери ЦВЗ можуть бути включені до складу принтерів, сканерів та інших приладів обробки даних. При несанкціонованій дії з документом, що містить ЦВЗ, такий прилад здатен блокувати виконання операції. Значною перевагою технології ЦВЗ є те, що вони подорожують разом із своїм контейнером по усій мережі і можуть витримувати деякі його трансформації, на відміну від звичайних метаданих, що часто губляться у процесі передачі. ЦВЗ також не потребують додаткового місця на друкованих матеріалах або упаковці та легко співіснує з, наприклад, магнітною стрічкою або штрихкодом.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

У кожного громадянина є персональний ідентифікатор, виданий країною для того, щоб підтвердити вашу особистість. Це може бути паспорт або водійські права. Цей документ використовується для доступу до широкого спектру послуг, включаючи подорожі, керування автомобілем, доступ до секретних будівель, банківські операції. Саме тому треба добре подбати про їх захист.

У сучасному світі ЦВЗ широко використовуються для захисту персональних ідентифікаторів; за їх допомогою можна швидко встановити справжність ідентифікатора та успішно боротися з їх крадіжками та підробками. Ідентифікатори скануються відповідними приладами на предмет наявності ЦВЗ, після чого легко можна зробити висновок про підробку документа [2].

ЗБЕРЕЖЕННЯ ДАНИХ, РОЗМІЩЕНИХ ОНЛАЙН

Відповідно до того, як користувачі стали все більше покладатися на Інтернет як засіб розповсюдження інформації, зв'язку з користувачами, досліджень та комунікації, об'єм даних, завантажених до мережі, росте з кожним днем.

Ким би ви не були: фотографом, розробником, художником, архівом – у вас є, чим поділитися з користувачами мережі. Проте, як тільки матеріали завантажено, ви ризикуєте втратити над ними контроль, тому що дуже важко відстежити, хто саме завантажив ваші матеріали і які дії над ними проводяться без вашого дозволу.

Якщо в матеріали, розміщені онлайн, інтегрувати ЦВЗ, згодом можна скористатися одним із сервісів для пошуку даних, що помічені саме цим унікальнім знаком. Після цього генерується звіт, що містить інформацію про поточне місцезнаходження даних, і володар може прийняти необхідні заходи. У випадку, коли матеріалів дуже багато і складно відстежити усі випадки власноруч, можливо налаштувати сервіс для передачі автоматичних повідомлень, наприклад:

- «Контент доступний для ліцензування»;
- «Контент захищений авторським правом. Будь ласка, негайно видаліть його»;
- «Відтворюємий контент захищений авторським правом і заборонений для програвання. Для більш детальної інформації відвідайте [веб-сайт]»;
- «Ви маєте дозвіл на використання цього контенту, проте ви повинні співвіднести його з власником та встановити посилання на [вебсайт]» [2].

ВІДСТЕЖЕННЯ ТРАНСЛЯЦІЙ

За останні роки кількість телевізійних і радіоканалів значно збільшилася, а отже, значно збільшився і потік контенту, що транслюється за допомогою цих каналів. У такій динамічній оточенні власнику контенту дуже важко ефективно управляти своїми медійними активами. Тому для правовласників, дистриб'юторів та трансляторів критично важливо мати точну інформацію про стан трансляцій. Проте як їм дізнатися, що відбувається із сигналом у момент, коли він покидає їх приміщення? Чи він взагалі передається? Чи використовується він згідно із контрактними домовленостями? Можливо, він змінений без відповідного дозволу? Для вирішення усіх цих питань використовується технологія ЦВЗ. За допомогою інтеграції такого знаку у відеоматеріал в момент його зняття або трансляції власник здатен безпомилково дізнатися, коли транслюють, де, хто і як довго.

Перевагою методу ЦВЗ при вирішенні задачі відстеження трансляції є його непомітність для людського ока, отже, його наявність ніяк не погіршує якості відеоматеріалу, що транслюється [1].

ЦВЗ можуть посилатися на базу даних, що містить більш повну інформацію згідно контенту. Метадані можуть містити будь-яку інформацію стосовно матеріалу, наприклад, його назву, формат, автора. У сфері відстеження трансляцій використовується спеціальне обладнання з метою моніторингу телеканалів та радіостанцій. При виявленні ЦВЗ дані швидко аналізуються, після чого генерується звіт із подробицями трансляції.

ЦИФРОВІ ВОДЯНІ ЗНАКИ У СФЕРІ МОБІЛЬНИХ ПРИСТРОЇВ

У наші часи мобільні телефони вже не використовуються лише для зв'язку; вони стали пристроєм, який знаходиться поруч із нами цілодобово і є джерелом допомоги, інформації та розваг. З плином часу смартфони стають дедалі потужнішими. Це призводить до потрясіння і значних

змін всередині підприємств. Газети і журнали шукають нові бізнес-моделі, які допоможуть їм залишатися актуальними і успішно функціонувати у майбутньому.

Технологія ЦВЗ надає великі можливості видавцям, брендам і маркетологам, що шукають шляхи приваблення споживачів за допомогою їх мобільних пристроїв. ЦВЗ можуть бути легко інтегровані до всіх типів медіа контенту, включаючи журнали, газети, плакати, брошури і т.д. На відміну від штрихкодів і QR-кодів, які використовувалися раніше, ЦВЗ є невидимими для людського ока і не займають місця на друкованих матеріалах, а також з легкістю «читаються» сучасними мобільними приладами [2].

ВИСНОВКИ

У зв'язку із бурхливим розвитком мультимедійних технологій гостро постало питання захисту авторських прав і інтелектуальної власності, представленої у цифровому вигляді. Переваги цифрового формату можуть бути переважені легкістю їх нелегальної зміни або копіювання.

Одним із найбільш успішних засобів захисту мультимедійної інформації полягає в інтеграції в захищаємий об'єкт невидимих для людського зору міток, так званих цифрових водяних знаків. Оскільки методи ЦВЗ почали розроблятися нещодавно, досі існує багато питань і проблем, що потребують вирішення. Проте уже зараз ця технологія використовується для розв'язання широкого спектру різноманітних задач.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ – М.: Вузовская книга, 2009. – 220 с.

2. Digital Watermarking Alliance (Електрон. ресурс) / Спосіб доступу: URL: www.digitalwatermarkingalliance.org

УДК 004.491

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ SETUP АТАКИ НА BITCOIN (ECDSA)

Шевченко Д.И.

Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: paiterofdreams@mail.ru

В работе рассматривается возможность клептографической атаки на Bitcoin (ECDSA).

Ключевые слова: *Bitcoin, ECDSA, клептография, SETUP.*

ВВЕДЕНИЕ

Bitcoin (биткойн) – пиринговая система электронной наличности, использующая одноимённую цифровую валюту, которую часто называют криптовалютой или виртуальной валютой. Сеть полностью децентрализована, не имеет центрального администратора или какого-либо его аналога [1].

Биткойны могут использоваться для оплаты товаров или услуг у продавцов, готовых их принимать. Есть возможность обмена на обычные деньги через специализированные площадки для торгов или пунктов обмена.

Одна из особенностей – эмиссия новых биткойнов. Она децентрализованная, лимитирована по объёму и времени, распределяется относительно случайно среди желающих, которые используют вычислительные мощности своего оборудования для защиты платёжной системы методом «proof-of-work» от повторного расходования средств.

Деятельность по обслуживанию системы с возможностью получить вознаграждение в форме эмитированных биткойнов и комиссионных сборов получила название «майнинга».

Базовым элементом этой платёжной системы является программа-клиент с открытым исходным кодом. С помощью сетевого протокола прикладного уровня запущенные на множестве компьютеров клиенты соединяются между собой в одноранговую сеть.

Для обеспечения функционирования и защиты системы используются криптографические методы [2].

SETUP АТАКА НА ECDSA

Термин «клептография» применяется для определения направления, связанного с использованием криптографии против криптографии. Клептографическая атака – это создание «закладки», внедряемой в разрабатываемую криптосистему. При этом, если рассматривать криптосистему как «черный ящик», невозможно определить, осуществил разработчик клептографическую атаку или нет. Метод похож на стеганографию, только внутри криптоалгоритмов [3].

Такой класс атак на криптоалгоритмы называется SETUP (Secretly Embedded Trapdoor with Universal Protection). То есть, обычно есть и «бэкдор» и защита, такая, что даже при обнаружении «бэкдора» невозможно будет узнать содержание передаваемых данных.

SETUP может быть слабым и сильным.

Weak SETUP – вариант, когда узнать сгенерированные ключи может не только атакующий, но и владелец устройства, на котором установлено скомпрометированное ПО.

Соответственно Strong SETUP – вариант, когда узнать ключи может только атакующий.

Еще одна характеристика называется «Leakage

bandwidth», она показывает сколько секретных данных «утекает» при повторяющемся процессе шифрования\подписи. Обозначается (m,n), что означает утечку m секретных сообщений/ключей за n передаваемых.

Такие атаки существуют практически для всех схем с открытым ключом. DSA, ElGamal, Diffie-Helman, везде есть способ передать скрытно какой-то объем информации. Далеко не всегда это получается легко, но при желании практическое применение найти можно. Например, для ECDSA провести SETUP атаку проще, потому что параметры генерации ключей (кривая, базовая точка, порядок кривой) известны заранее, а в DSA соответствующие параметры генерируются случайным образом для каждой ключевой пары.

Как известно, кошелек в Bitcoin – это ключевая пара ECDSA.

Рассмотрим сильную SETUP атаку (1,2) на ECDSA, то есть атакующий может узнать секретный ключ пользователя за 2 подписи, при чем, кроме него никто это сделать не сможет.

Для начала приведем упрощенную процедуру генерации подписи ECDSA.

1. Есть закрытый ключ d – число и открытый ключ Q – точка эллиптической кривой, равная dG, где G – базовая точка кривой.

2. Для подписи выбирается случайное число k, в диапазоне [1, n-1].

3. Вычисляется точка кривой (x1 y1) = k*G

4. Вычисляется r = x1 mod N, где N – порядок кривой.

5. Вычисляется s = k-1(H(m)+rd) mod N, где k-1 – число, обратное по модулю N к k. H(m) – хэш подписываемого сообщения.

Подписью является пара (r,s).

Как видно, тут k выбирается случайно. Немного видоизменим процесс так, чтобы атакующий смог вычислить секркткный ключ пользователя d.

Закрытый и открытый ключи атакующего назовем v и V = vG.

Шаг первый (неизменный). Пользователь генерирует подпись первый раз (отправляет кому-то биткоины)

Идентичный обычной подписи за тем исключением, что понадобится где-то сохранить k. Назовем его k1. Получаем пару (r1, s1).

Шаг второй (отправляет биткоины второй раз)

Вычисляем скрытый элемент поля

$$Z = a*k1\ G + b*k1\ V + h*jG + e*uV, \quad (1)$$

где a, b, h, e <n − фиксированные целые числа; j, u ∈ {0, 1} – случайные.

Параметры a, b, h, e можно генерировать детерминировано, например, используя хэш от сообщения как seed для ГПСЧ (генератор псевдослучайных чисел). Это усложнит обнаружение закладки.

Параметр k2 выбирается не случайно, а является теперь хэшем от Z. Хэшем от точки кривой будем считать хэш её X координаты.

Далее всё как обычно, получаем пару (r2, s2).

Итак, атакующий получил пары (r1, s1) и (r2, s2). Приведем алгоритм получения закрытого ключа пользователя.

1) Вычисляем

$$R1' = s\text{-}1(H(m1)G + r1Q) = (x1\ ', y1\ ') \quad (2)$$

Проверяем цифровую подпись.

2) $$Z1 = aR1' + b * vR1', \quad (3)$$

где v – закрытый ключ атакующего

3) Для каждого возможного значения j, u вычисляем:

$$Z2 = Z1 + h * jG + e * uV \quad (4)$$

$$k2' = H\ (Z2) \quad (5)$$

$$R2' = k2'G = (x2', y2') \quad (6)$$

$$r2' = x2' \bmod n \quad (7)$$

Если r2′ = r2, тогда k2′ = k2, найдено k, что и являлось целью.

Закрытый ключ пользователя

$$d= (s2k2 - h(m2)) \times r2\text{-}1 \bmod n \quad (8)$$

Параметр k2 тоже можно запомнить и продолжить генерировать k+1 по цепочке, давая таким образом атакующему возможность узнать закрытый ключ пользователя по любым двум идущим подряд подписям [4].

Ничего необычного тут нет, атакующему лишь нужно заранее выбрать числа a, b, h, e и поместить их в «бекдор» вместе со своим открытым ключом либо генерировать их на основе подписываемого сообщения.

ВЫВОД

Сама атака хоть и сильная, но неустойчивая. Это означает, что пользователь, владеющий своим закрытым ключом, теоретически может вычислить, что k2 генерируется неслучайным образом. Для этого и вводятся j,u, чтобы разнообразить возможные значения на случай проверки бдительным пользователем. Их можно сделать отличными от 0 и 1, тогда вариантов будет еще больше. Но в этом случае полный перебор займет намного больше времени. Однако, эта атака в большинстве случаев выявляется слишком поздно, что обуславливает актуальность ее нейтрализации.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Биткойн (Электрон. ресурс) / Способ доступа: URL: https://ru.wikipedia.org/wiki/Биткойн – Загол. с экрана.
2. Биткойн: система цифровой пиринговой наличности (Электрон. ресурс)/ Способ доступа: URL: https://bitcoin.org/bitcoin_ru.pdf – Загол. с экрана.
3. Клептографические атаки на криптосистемы с открытым ключом (Электрон. ресурс)/ Способ доступа: URL: http://www.aha.ru/~msa/papers3.pdf- Загол. с экрана.
4. Встраиваем бэкдор в Bitcoin (ECDSA) или еще раз о клептографии (Электрон. ресурс)/ Способ доступа: URL: http://habrahabr.ru/post/248419/– Загол. с экрана.

УДК: 004.896

ОСОБЕННОСТИ ПРИМЕНЕНИЯ НЕЙРОКОМПЬЮТЕРОВ

Палий В.В.[1], Макаров А.С.[2]
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: coolvpal@gmail.com[1], sasasasha@ukr.net[2]

В данной статье рассмотрены нейрокомпьютеры, их применение в современном мире, в частности, в криптографии (блочный шифр AES-128)

Ключевые слова: нейрокомпьютер, коннекционизм, нейропроцессор.

ВСТУПЛЕНИЕ

Нейрокомпьютер — устройство переработки информации на основе принципов работы естественных нейронных систем.[1] Эти принципы были формализованы, что позволило говорить о теории искусственных нейронных сетей. Проблематика же нейрокомпьютеров заключается в построении реальных физических устройств, что позволит не просто моделировать искусственные нейронные сети на обычном компьютере, но так изменить принципы работы компьютера, что станет возможным говорить о том, что они работают в соответствии с теорией искусственных нейронных сетей.

В отличие от цифровых систем, представляющих собой комбинации процессорных и запоминающих блоков, нейропроцессоры содержат память, распределённую в связях между очень простыми процессорами, которые часто могут быть описаны как формальные нейроны или блоки из однотипных формальных нейронов. Тем самым основная нагрузка на выполнение конкретных функций процессорами ложится на архитектуру системы, детали которой в свою очередь определяются межнейронными связями. Подход, основанный на представлении как памяти данных, так и алгоритмов системой связей (и их весами), называется коннекционизмом. [2]

Три основных преимущества нейрокомпьютеров:

1. Все алгоритмы нейроинформатики высокопараллельны, а это уже залог высокого быстродействия.
2. Нейросистемы можно легко сделать очень устойчивыми к помехам и разрушениям.
3. Устойчивые и надёжные нейросистемы могут создаваться и из ненадёжных элементов, имеющих значительный разброс параметров. [3]

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

В результате проведенных исследований было установлено, что основными сферами применения нейрокомпьютеров являются:

1. Управление в реальном времени, в том числе:
- самолётами и ракетами,
- технологическими процессами непрерывного производства (в энергетике, металлургии и др.),
- гибридными двигателями автомобиля,
- пневмоцилиндром,
- сварочным аппаратом,
- электропечью,
- турбогенератором.

2. Распознавание образов:
- изображений, человеческих лиц, букв и иероглифов, отпечатков пальцев в криминалистике, речи, сигналов радара и сонара,
- элементарных частиц и происходящих с ними физических процессов (эксперименты на ускорителях или наблюдение за космическими лучами),
- заболеваний по симптомам (в медицине),
- местностей, где следует искать полезные ископаемые (в геологии, по косвенным признакам),
- признаков опасности в системах защиты информации.

3. Прогнозирование в реальном времени:
- погоды,
- курса акций (и других финансовых показателей),
- исхода лечения,
- политических событий (результатов выборов, международных отношений и др.),
- поведения противника (реального или потенциального) в военном

4. Протезирование («умные протезы») и усиление естественных функций, в том числе — за счёт прямого подключения нервной системы человека к компьютерам (Нейрокомпьютерный интерфейс).
5. Психодиагностика
6. Телекоммуникационное мошенничество, его обнаружение и предотвращение с помощью нейросетевых технологий — по мнению некоторых специалистов являются одной из самых перспективных технологий в области защиты информациии в телекоммуникационных сетях. [4]
7. Криптоанализ шифров, таких как AES. Рассмотрим взлом шифра AES-128 (количеством раундов 10) его взлом одним процессором Intel Core i7 5960x (производство 2014 г.298,190 MIPS при 3.0 GHz). Чтобы посчитать мы узнаем количество нужных IPS для его взлома методом «Brute force» (1).

$$IPS_1 = 2^{128} \times 10 \quad (1)$$

где IPS_1 - количество нужных операций для взлома. Время на взлом T будет равняться(2):

$$T = \frac{(2^{128} \times 10)}{298.190 \times 10^6} \approx 35.96 \times 10^{19} \text{ (лет)} \quad (2)$$

При этом если мы будем увеличивать количество процессоров, то мы увеличиваем призводительность линейно. Но если попробуем использовать процессор, например, это Ni1000 (разработка фирмы Intel совместно с Nestor, имитирующих 1024 нейрона, быстродействие 33 МГц, 17 GIPS, то при увеличении

вдвое производительность увеличится в 5-8 раз (при использовании гарвардской архитектуры).

Соответственно при использовании 10 обычных процессоров мы получим:

$$T = \frac{(2^{128} \times 10)}{298.190 \times 10^{6} \times 10} \approx 35.96 \times 10^{18} \text{ (лет)} \quad (3)$$

где Т – время взлома

При использовании нейронных (4):

$$T = \frac{(2^{128} \times 10)}{17 \times 10^{9} \times 5^{10}} \approx 64.99 \times 10^{13} \text{ (лет)} \quad (4)$$

ВЫВОД

Нейрокомпьютеры являются очень перспективными в наше время, ведь задачи, предстающие человечеством, становятся все сложнее, а ресурсов на их решения нам не хватает. Именно поэтому стоит положиться на аналог человеческого мозга, заключенного в машине.

СПИСОК ИСТОЧНИКОВ

1. Дунин-Барковский В. Л., Нейрокибернетика, Нейроинформатика, Нейрокомпьютеры, В кн.: Нейроинформатика / А. Н. Горбань, В. Л. Дунин-Барковский, А. Н. Кирдин и др. — Новосибирск: Наука. Сибирское предприятие РАН, 1998. — 296 с ISBN 5-02-031410-2

2. Винер Н., Кибернетика, или Управление и связь в животном и машине. / Пер. с англ. И. В. Соловьева и Г. Н. Поварова; Под ред. Г. Н. Поварова. — 2-е издание. — М.: Наука, 1983. — 344 с.

3. Горбань А. Н. Нейрокомпьютер, или Аналоговый ренессанс, Мир ПК, 1994, № 10, 126—130.

4. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. и др. Применение искусственных нейронных сетей и системы остаточных классов в криптографии,- М.: ФИЗМАТЛИТ, 2012.- 280 с. - ISBN: 978-5-9221-1386-

УДК 351.862.4:327:004.056

ПРОГРАМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УКРАЇНІ

Ізмалков Олексій Миколайович

Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,

http://bit.nmu.org.ua, E-mail:Elena-izmal@rambler.ru

В роботі відображені основні проблеми забезпечення інформаційної безпеки України, сформульовані основні цілі щодо підвищення рівня захисту інформаційних ресурсів держави та запропоновані програми по досягненню цих цілей.

Ключові слова – інформаційна безпека держави; атака на інформаційну систему; виявлення атак і несанкціонованих вторгнень; програма

ВСТУП

Менше, ніж за одне покоління інформаційна революція і впровадження комп'ютерних технологій фактично в кожну сферу життя суспільства призвели до принципово нових досягнень у сфері управління економікою, забезпечення національної безпеки, значно підвищили комфортність нашого повсякденного життя.

Всі системи, керовані комп'ютерами, уразливі відносно вторгнень і руйнувань. Узгоджена атака на інформаційну систему будь-якого ключового економічного сектора або урядової установи може мати катастрофічні наслідки. Сьогодні портативний комп'ютер в руках кримінальних елементів або терористів може перетворитися на сильну зброю, здатну привести до величезних руйнувань. В даний час питання забезпечення безпеки інформаційних систем найактуальніша. Конфлікт на сході України та суттєві проблеми з інформаційною безпекою наразі є головною проблемою держави. Україна повинна розпочати дискусію із залученням експертів з інформаційної безпеки, журналістів та медіа-експертів з Великобританії, Польщі, країн Балтії та США для початку вирішення питань з інформаційної безпеки. На базі отриманого досвіду та аналізу закордонних інформаційних систем потрібно створити програми для забезпечення інформаційної безпеки держави в Україні.

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Для вирішення проблем в галузі забезпечення інформаційної безпеки потрібне вдосконалення підходів до захисту інформаційних ресурсів на державному рівні. Для цього визначені три основні мети.

1 Підготовка до інформаційної атаки та мінімізація її наслідків. Дана мета передбачає реалізацію кроків, необхідних для мінімізації можливості істотних атак на основні інформаційні мережі України та побудови інфраструктури, стійкої до таких атак. Результатом її виконання буде поетапний захист інформаційних систем та зменшення можливості проведення атак на них;

2 Забезпечення швидкого реагування та протидія несанкціонованим вторгненням. Ця мета передбачає здійснення дій, необхідних для своєчасного визначення та оцінки нападу, його стримування, швидкого відновлення після вторгнення та відтворення ураженої системи. Реалізація цієї мети дозволить збільшити швидкість реагування на атаку та протидії їй. Відмінність першої мети від другої в тому, що досягнення першої мети дозволить зменшити тільки наслідки інформаційної атаки, а другої - забезпечить протидію та швидке реагування на неї;

3 Захист інформаційної системи на державному рівні - це те, що Україна повинна зробити для створення організаційної, кадрової та законодавчої підтримки запропонованих заходів, тобто те, що, в кінцевому рахунку, зробить інформаційну

інфраструктуру і працюючих у цій сфері фахівців здатними запобігти, виявити і відреагувати на вторгнення в критичні інформаційні мережі[1-3].

Для досягнення вказаних цілей пропонується до реалізації 8 програм.

Для реалізації першої мети «Підготовка до інформаційної атаки та мінімізація її наслідків» пропонується Програма 1: «Визначення основних компонентів та інформаційних ресурсів інфраструктури держави», яка призначена як для державного, так і для приватного сектора. Вона дає можливість визначити найбільш істотні компоненти, взаємозалежності і вразливості основних інформаційних мереж, які можуть піддатися нападу, а також розробити і реалізувати заходи з усунення вразливостей. При цьому програма передбачає постійне оцінювання стану даних систем і усунення несправностей.

Перший необхідний крок у підготовці та здійсненні заходів захисту інформаційних систем - повна оцінка інформаційних ресурсів, якими вони оперують, їх основних компонентів, взаємозалежностей між ними та їх вразливостей.

Ключовими моментами такого визначення є:

- аналіз загальних взаємозалежностей в межах державних структур або між державним і приватним сектором;

- оцінка вразливостей мережі адміністраторами систем, операторами, фахівцями з безпеки, заснована на ідентифікації основних інформаційних ресурсів і компонентів, а також загальних взаємозалежностей;

- оцінка вразливостей різних систем сторонніми фахівцями.

Для досягнення другої мети «Забезпечення швидкого реагування та протидія несанкціонованим вторгненням» пропонуються дві програми.

Програма 2: «Виявлення атак і несанкціонованих вторгнень» передбачає встановлення багатоступеневого захисту комп'ютерних систем, включаючи системи виявлення вторгнень, ідентифікатори аномального режиму роботи, корпоративні системи управління та сканери зловмисних кодів.

План реалізації цієї програми передбачає застосування кращих сучасних типів захисних систем.

Програма 3: «Вдосконалення діяльності розвідувальних служб і застосування нормативно-правових заходів для захисту основних інформаційних систем» орієнтована на вдосконалення діяльності та зміцнення правоохоронних органів і розвідувальних служб. Підвищення рівня їх обізнаності з засобів протидії новим видами загроз та зловмисникам, націленим на інформаційні системи України.

Дана програма констатує, що несанкціоноване вторгнення в комп'ютерні мережі є грубим порушенням законів України [1-2].

Доказ, що атака мала місце, з'ясування, хто це зробив, а також доказ провини зловмисників вимагають нових навичок, які потребують об'єднання ресурсів правоохоронних органів і потужних аналітичних служб національної безпеки.

Досягнення мети «Захист інформаційної системи на державному рівні» пропонується за рахунок впровадження п'яти наступних програм.

Програма 4: «Розширення науково-дослідних робіт в підтримку програм 1-3» встановлює вимоги до досліджень, визначає порядок фінансування робіт і систему, яка гарантує розробку технологій забезпечення інформаційної безпеки на випередження новим інформаційним загрозам.

В програмі виділено такі пріоритетні напрямки наукових досліджень та розробок:

- технології створення та підтримки функціонування моніторів виявлення вторгнень до великомасштабних мереж;

- використання систем штучного інтелекту та інших методів виявлення програмних закладок в операційній системі;

- методології організації інформаційних систем, здатних стримати, зупинити або вигнати зловмисників із системи, зменшити пошкодження або відновити служби обробки інформації в разі нападу або катастрофи.

Програма 5: «Підготовка необхідної кількості фахівців у галузі інформаційної безпеки» визначає кількість людей і навички, якими повинні володіти фахівці в галузі інформаційної безпеки, що працюють як в апараті Президента, так і в цілому по країні в національному масштабі. Крім того, вона передбачає підготовку службовців, навчання та наймання на роботу додаткового персоналу для заповнення нестачі кваліфікованих кадрів.

Програма 6: «Підвищення рівня обізнаності громадян України в питаннях інформаційної безпеки» націлена на реалізацію низки заходів, покликаних пояснити громадськості необхідність діяти негайно, запобігаючи катастрофу, підвищувати здатність ефективно протидіяти навмисним нападам на інформаційні системи. У своїй початковій стадії програма передбачає для цього реалізацію, принаймні, трьох наступних елементів:

- навчання української молоді інформаційній етиці, відповідній поведінці при користуванні Internet та іншими засобами комунікацій;

- забезпечення співпраці з європейськими державами та отримання досвіду із захисту інформаційних систем для вдосконалення національної «кібербезпеки» в приватному секторі і в уряді;

- досягнення того, щоб службовці самі були зразком розуміння потреби в забезпеченні інформаційної безпеки систем.

Четвертий елемент може бути доданий з часом. Він передбачає поширення кампанії розуміння необхідності забезпечення інформаційної безпеки на інші приватні організації та на всю громадськість.

Програма 7: «Прийняття законодавчих актів і виділення асигнувань на підтримку програм 1-6» передбачає розвиток законодавчої бази, необхідної для підтримки ініціатив, запропонованих в інших програмах. Ця діяльність вимагає інтенсивної співпраці між органами державної влади і приватним сектором економіки.

Програма 8: «Забезпечення надійної гарантії

повного захисту громадянських свобод українських громадян, їх права на секретність і на захист персональних даних» включена в усі інші програми і визначає те, що необхідно робити для захисту основних інформаційних систем відповідно до конституційного та інших законних прав громадян України[3].

ВИСНОВКИ

Застосування запропонованих програм дозволить Україні забезпечити захист своїх інформаційних систем і ресурсів задля збереження своєї зовнішньої та внутрішньої безпеки, вирішення державних та адміністративних проблем в галузі інформаційної безпеки, а саме забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів держави.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю // Право України. – 2002. - № 5. – С.121-126.
2. Про Доктрину інформаційної безпеки України: Указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіц. вісник України. – 2009. – № 52. – Ст. 1783. – С. 7. – 20 лип
3. "Про виклики та загрози національній безпеці України у 2011 році" : Указ Президента України від 10 груд. 2010 р. № 1119/2010

УДК 004.056

УЯЗВИМОСТЬ ПРОТОКОЛА WPS В БЕСПРОВОДНЫХ СЕТЯХ WI-FI

Амиров Николай Гурамович
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: kenobi@ukr.net

В протоколе WPS существует уязвимость, которая позволяет свести взлом беспроводной точки Wi-Fi к методу полного перебора за допустимое время.

Ключевые слова – несанкционированный доступ, беспроводные сети, WPS, метод полного перебора.

ВВЕДЕНИЕ

Протокол WPS (Wi-Fi Protected Setup) был разработан для маршрутизаторов с целью упрощения настройки и подключения к защищенной беспроводной сети. Однако, в WPS была обнаружена уязвимость, сводящая защиту сети к минимуму.

ПРИНЦИП РАБОТЫ WPS

Механизм автоматически задает имя сети и шифрование. Таким образом, пользователю нет необходимости самостоятельно конфигурировать маршрутизатор. Все, что требуется клиенту для получения необходимых данных – это ввод корректного восьмизначного PIN кода [1].

УЯЗВИМОСТЬ WPS

Поскольку PIN код состоит из восьми цифр, то существует 10^8 = 100 000 000 вариантов для полного перебора.

Однако первые семь цифр PIN кода являются случайными, а восьмая – представляет собой контрольную сумму первых семи.

IEEE 802.11			
	Запрашивающее устр-во → Точка доступа	**Запрос аутентификации**	**802.11 Аутентификация**
	Запрашивающее устр-во ← Точка доступа	**Ответ на запрос**	
	Запрашивающее устр-во → Точка доступа	**Запрос ассоциации**	**802.11 Ассоциация**
	Запрашивающее устр-во ← Точка доступа	**Ответ на запрос**	
IEEE 802.11/EAP			
	Запрашивающее устр-во → Точка доступа	**Запуск EAPOL**	**Инициализация EAP**
	Запрашивающее устр-во ← Точка доступа	**EAP - запрос идентификатора**	
	Запрашивающее устр-во → Точка доступа	**EAP - посылка идентификатора**	
IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Запрашивающее устр-во →Устройство-регистратор	N1 || **Описание** || PK_E	**Ключевой обмен по методу Диффи-Хеллмана**
M2	Запрашивающее устр-во ←Устройство-регистратор	N1 || N2 || **Описание** || PK_R || **Аутентификатор**	
M3	Запрашивающее устр-во →Устройство-регистратор	N2 || E-Hash1 || E-Hash2 || **Аутентификатор**	
M4	Запрашивающее устр-во ←Устройство-регистратор	N1 || R-Hash1 || R-Hash2 || $E_{KeyWrapKey}$(R-S1) || **Аутентификатор**	**Доказательство обладания 1ой половиной PIN-кода**
M5	Запрашивающее устр-во →Устройство-регистратор	N2 || $E_{KeyWrapKey}$(E-S1) || **Аутентификатор**	**Доказательство обладания 1ой половиной PIN-кода**
M6	Запрашивающее устр-во ←Устройство-регистратор	N1 || $E_{KeyWrapKey}$(R-S2) || **Аутентификатор**	**Доказательство обладания 2ой половиной PIN-кода**
M7	Запрашивающее устр-во →Устройство-регистратор	N2 || $E_{KeyWrapKey}$(E-S2 || **Данные конфигурации**) || **Аутентификатор**	**Доказательство обладания 2ой половиной PIN-кода**
M8	Запрашивающее устр-во ←Устройство-регистратор	N1 || $E_{KeyWrapKey}$(**Данные конфигурации**) || **Аутентификатор**	**Конфигурация точки доступа**

Рисунок 1. Протокол аутентификации WPS

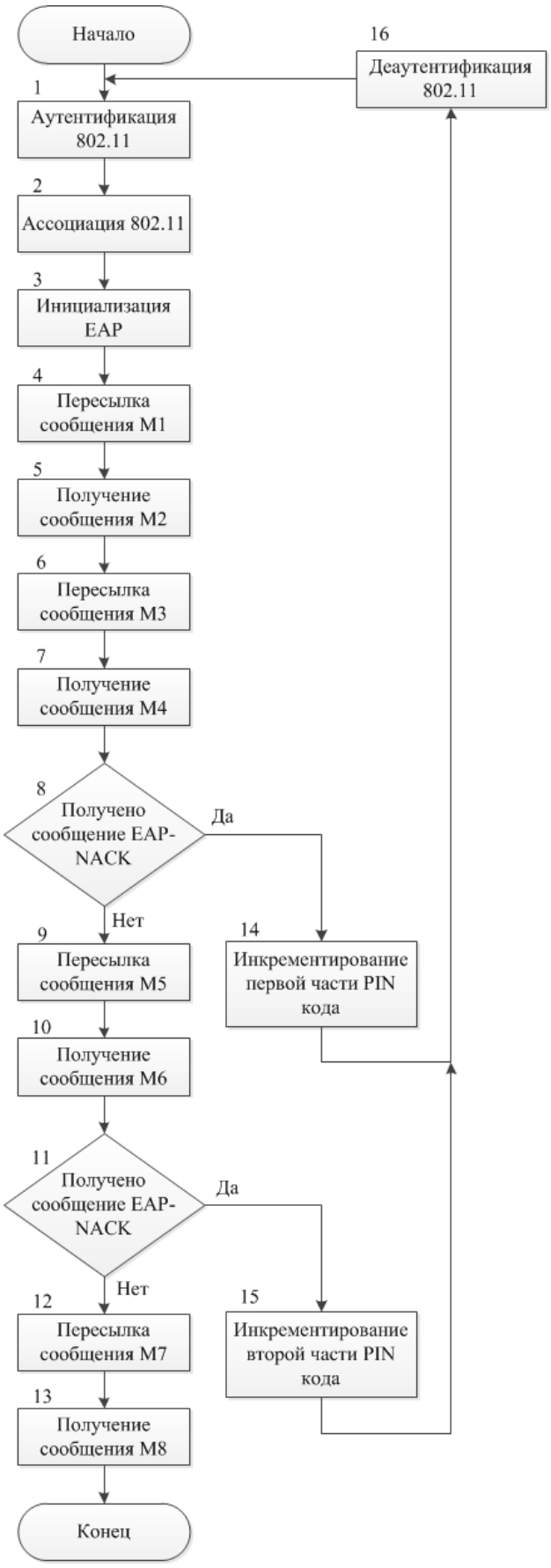


Рисунок 2. Общая схема перебора PIN кодов

Таким образом, для метода полного перебора остается 10^7 = 10 000 000 вариантов [1].

Как видно из протокола аутентификации WPS (рисунок 1), при проверке PIN код делится на две равные части, каждая из которых обрабатывается отдельно. Таким образом, если после отсылки сообщения M4 маршрутизатор отвечает кодом EAP-NACK, то это означает, что первая часть PIN кода не верна. Если же маршрутизатор отвечает кодом EAP-NACK после отсылки сообщения M6, то это означает, что вторая часть PIN кода не верна. [2]

Исходя из этого, остается лишь 10^4 = 10000 вариантов перебора для первой части PIN кода и 10^3 = 1000 вариантов для второй, что в сумме дает 11000 вариантов для неизбежного нахождения верного PIN кода и получения доступа к беспроводной сети (рисунок 2) [1].

Возможная скорость перебора при этом может быть ограничена скоростью обработки маршрутизатором WPS-запросов. Основное время при этом затрачивается на расчет открытого ключа по алгоритму Диффи-Хеллмана, он должен быть сгенерирован перед отсылкой сообщения M3 [1].

ВЫВОД

Протокол WPS чрезвычайно уязвим для атаки методом полного перебора. Единственным способом защититься является отключение протокола WPS на маршрутизаторе, либо же блокировка функций WPS на некоторое время после нескольких неудачных попыток ввода PIN кода. Однако, второй вариант лишь замедлит атакующего, но не устранит угрозу в целом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Журнал Хакер, Март (03) 158.

2. Энциклопедия теоретической и прикладной криптографии: Обеспечение безопасности беспроводных сетей/ (Электронный ресурс) / способ доступа: http://cryptowiki.net/index.php?title= Обеспечение_безопасности_беспроводных_сетей

УДК 004.91:65.012.8

ОБЩИЕ И ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

Щербакова Анна Евгеньевна[1], Тимофеев Дмитрий Сергеевич
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: annascherbakova03@gmail.com[1]

В данной статье рассматриваются общие и организационные требования к защите информации в автоматизированных системах предприятия от несанкционированного доступа. Также показан перечень основных требований к защите информации, описаны способы по ограничению доступа к информации.

Ключевые слова: несанкционированный доступ (НСД), утечка информации, система защиты информации (СЗИ), требования к защите информации, средства вычислительной техники (СВТ), информационная система (ИС), автоматизированная система (АС).

ВСТУПЛЕНИЕ

Информационная безопасность предприятия в настоящее время является одной из самых важных составляющих безопасности предприятия в целом. Ее обеспечение становится все более сложным и значимым процессом. Безопасность информации – это не только защита от утечки, но и обеспечение ее сохранности, а также меры по защите важнейших данных от несанкционированного доступа и обеспечению доступности информации в случае форс-мажорных обстоятельств. Основные ее составляющие: конфиденциальность, целостность, доступность.

ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

Требования по защите информации определяются владельцем ИС и согласовываются с исполнителем работ по созданию системы защиты информации (исполнитель должен иметь соответствующую лицензию на право проведения таких работ).

В процессе формирования требований к системе защиты информации целесообразно найти ответы на следующие вопросы:

1. Какие меры безопасности предполагается использовать?
2. Какова стоимость доступных программных и технических мер защиты?
3. Насколько эффективны доступные меры защиты?
4. Насколько уязвимы подсистемы СЗИ?
5. Имеется ли возможность провести анализ риска (прогнозирование возможных последствий, которые могут вызвать выявленные угрозы и каналы утечки информации)?

СОВОКУПНОСТЬ ТРЕБОВАНИЙ К СИСТЕМАМ ЗАЩИТЫ ИНФОРМАЦИИ

В общем случае целесообразно выделить следующие группы требований к системам защиты информации:

- общие требования;
- организационные требования;
- конкретные требования к подсистемам защиты, техническому и программному обеспечению, документированию, способам, методам и средствам защиты.

ОБЩИЕ ТРЕБОВАНИЯ

Прежде всего, необходима полная идентификация пользователей, терминалов, программ, а также основных процессов и процедур, желательно до уровня записи или элемента. Также следует ограничить доступ к информации, используя совокупность следующих способов:

- иерархическая классификация доступа;
- классификация информации по важности и месту ее возникновения;
- указание ограничений к информационным объектам, например, пользователь может осуществлять только чтение файла без права записи в него;
- определение программ и процедур, предоставленных только конкретным пользователям.

Система защиты должна гарантировать, что любое движение данных идентифицируется, авторизуется, обнаруживается и документируется. Обычно формулируются общие требования к следующим характеристикам:

- способам построения СЗИ либо ее отдельных компонент (к программному, программно-аппаратному, аппаратному);
- архитектуре СЗИ и ИС;
- применению стратегии защиты;
- затратам ресурсов на обеспечение СЗИ (к объемам дисковой памяти для программной версии и оперативной памяти для ее резидентной части, затратам производительности вычислительной системы на решение задач защиты);
- надежности функционирования СЗИ (к количественным значениям показателей надежности во всех режимах функционирования ИС и при воздействии внешних разрушающих факторов, к критериям отказов);
- количеству степеней секретности информации, поддерживаемых СЗИ;
- обеспечению скорости обмена информацией в ИС, в том числе с учетом используемых криптографических преобразований;
- количеству поддерживаемых СЗИ уровней полномочий;

- возможности СЗИ обслуживать определенное количество пользователей;
- продолжительности процедуры генерации программной версии СЗИ;
- продолжительности процедуры подготовки СЗИ к работе после подачи питания на компоненты ИС;
- возможности СЗИ реагировать на попытки несанкционированного доступа, либо на “опасные ситуации”;
- наличию и обеспечению автоматизированного рабочего места администратора защиты информации в ИС;
- составу используемого программного и лингвистического обеспечения, к его совместимости с другими программными платформами
- к возможности модификации и т.п.;
- используемым закупаемым компонентам СЗИ (наличие лицензии, сертификата и т.п.).

ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ

Организационные требования к системе защиты предусматривают реализацию совокупности административных и процедурных мероприятий. Требования по обеспечению сохранности должны выполняться, прежде всего, на административном уровне. Организационные мероприятия, проводимые с целью повышения эффективности защиты информации, должны предусматривать следующие процедуры:

- ограничение несопровождаемого доступа к вычислительной системе (регистрация и сопровождение посетителей);
- осуществление контроля за изменением в системе программного обеспечения;
- выполнение тестирования и верификации изменений в системе программного обеспечения и программах защиты;
- организацию и поддержку взаимного контроля за выполнением правил защиты данных;
- ограничение привилегии персонала, обслуживающего ИС;
- осуществление записи протокола о доступе к системе;
- гарантию компетентности обслуживающего персонала;
- разработку последовательного подхода к обеспечению сохранности информации для всей организации;
- организацию четкой работы службы ленточной и дисковой библиотек;
- комплектование основного персонала на базе интегральных оценок и твердых знаний;
- организацию системы обучения и повышения квалификации обслуживающего персонала.

Служба безопасности занимается и разработкой организационно-распорядительных документов и контролирует их выполнение. Особое внимание уделяется допуску и доступу сотрудников предприятия к конфиденциальной информации, проверке носителей информации. В результате проведение организационных мероприятий позволяет перекрыть большую часть каналов утечки информации и объединить используемые специализированные средства защиты в единый механизм. Совокупность организационных методов и специализированных средств защиты позволяет оперативно реагировать на угрозы в процессе хранения, обработки, передачи информации, а также обеспечивать ее доступность и целостность. Только при совместном их применении достигается наилучший результат. По окончании проведения мероприятий по защите, а также в процессе эксплуатации АС проводится оценка эффективности средств защиты, при которой используется преимущественно системный подход. При этой оценке необходимо учитывать общие технические характеристики объекта защиты (включая практическую реализацию средств защиты), а также экономическую сторону данного вопроса. Необходимо осуществлять контроль эффективности средств защиты от НСД, который может производиться либо периодически, либо по мере необходимости. В случае необходимости выполняется доработка средств защиты.

ВЫВОД

Техническим средствам защиты информации нужна непрерывная организационная поддержка, которая заключается в смене паролей, определении ролей, полномочий, разграничении доступа и т. п. То есть защита информации – это не разовое мероприятие, это постоянный процесс. Требуется обеспечить беспрерывность работы средств защиты, чтобы злоумышленники не смогли проанализировать систему безопасности и при случае воспользоваться возможными уязвимостями, заложить «закладки» или вывести систему из строя. В результате проведение организационных мероприятий позволяет перекрыть большую часть каналов утечки информации и объединить используемые специализированные средства защиты в единый механизм.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ “Про Положення про технічний захист інформації в Україні” від 06.10.2000 р.

2. ЗАКОН УКРАЇНИ “Про інформацію” від 30.10.1997 р.

3. НД ТЗІ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі”

4. НД ТЗІ 1.1-002-99 “Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу”

УДК 65.011.3

АНАЛІЗ FREAK АТАКИ ЧЕРЕЗ ВРАЗЛИВІСТЬ «CVE-2015-0204»

Колгін Володимир Андрійович[1], Масальська Олена Олександрівна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: vovik425@gmail.com[1]

Ця стаття призначена для ознайомлення з новою атакою на основі MITM-атаки, аналіз її реалізації, алгоритм та умови атаки.

Ключові слова – MITM-атака, HTTPS-протокол, OpenSSL

ВСТУП

Дослідники з INRIA (національний дослідницький інститут у Франції, що працює в галузі комп'ютерних наук, теорії управління та прикладної математики) і Microsoft повідомили про виявлення уразливості під номером CVE-2015-0204, яка, імовірно, існувала протягом більш ніж 15 років і яка робить технічно можливим перехоплення HTTPS-трафіку, який йде між певними сайтами і пристроями під керуванням Apple iOS і MacOS, а також Google Android.

FREAK - це абревіатура від Factoring attack on RSA-EXPORT Keys. Атака спрацьовує, коли вразливі пристрої підключаються до сайтів, на яких стоїть морально застаріле програмне забезпечення для шифрування, яке, як вважалося, вже давно ніким не використовується. Зловмисник, який має можливість перехоплювати трафік між вразливим пристроєм і вразливим сервісом, може впровадити в нього свої спеціальним чином створені пакети, які змусять обидві сторони використовувати "для спілкування" слабкий 512-розрядний ключ для шифрування. Змусити браузер і сайт перейти на більш низький рівень шифрування - ключовий момент FREAK-атаки.

Після цього зловмисник може використовувати орендовані на, наприклад, Amazon, обчислювальні потужності для того, щоб легко дешифрувати слабкий за нинішніми мірками ключ, схований у перехопленій трафіку. За оцінками фахівців, вартість потужностей, потрібних для такої операції складає близько 100 доларів, що робить FREAK привабливим для хакерів-аматорів, а професіоналам дозволяє поставити злом "на потік". Розкривши ключ, зловмисник може "підняти" в локальній мережі або, наприклад, в Wi-Fi-мережі кафе, копію даного його сайту і збирати різну інформацію - логіни і паролі від соціальних мереж, ключі від інтернет-банків і так далі.

Попутно вимальовується кілька додаткових проблем, які роблять FREAK дуже ефективною атакою. По-перше, генерувати нові RSA-ключі - дороге задоволення, тому багато веб-сервери, стартуючи, генерують один єдиний ключ, який потім використовують для захисту всіх з'єднань. Якщо зловмисник його перехоплює - він може ним користуватися "всю дорогу".

По-друге, HTTPS-протокол не вимагає від учасників з'єднання відмови від використання 512-бітних ключів, в результаті чого останній є цілком "валідним" для спілкування між сервером і клієнтом. Навіть, незважаючи на те, що сучасні обчислювальні потужності дозволяють його зламати хакерам-любителям за розумний час.

ПРИЧИЕВ ВИНИКНЕННЯ УЯЗЛИВОСТІ

Адміністрація президента Білла Клінтона, яка в 1990-х роках заборонила експортувати з США криптографічні алгоритми та пристрої певної "потужності". В результаті слабкий 512-розрядний ключ став стандартом де-факто - і залишається ним навіть сьогодні, коли заборони на експорт криптографічних технологій вже давно немає. Стандартом він став просто тому, що спочатку всі хотіли, щоб з їх сайтами і технологіями взаємодіяло якомога більше людей, включаючи і іноземців, позбавлених криптографічної мощі США.

УМОВИ АТАКИ

З'ясувалося, що в реалізації OpenSSL (Браузер в Android) і Apple TLS / SSL (Safari) існує баг, який дозволяє «людині посередині» змусити клієнта використовувати EXPORT-шифрування, навіть якщо клієнт не заявляв про його підтримку. Для цього повинні виконуватися відразу декілька умов:

Клієнт використовує вразливу версію OpenSSL або Apple TLS / SSL

Підтримка EXPORT-шифрування включена на сервері

Наявність закритого ключа RSA 512 біт у зловмисника

Для того, щоб експлоїт спрацював, вразливе пристрій повинен підключатися до уразливого сайту. І "спілкування" між ними повинно проходити в мережі, до якої у зловмисника є доступ. Якщо Ваш пристрій не вразливий, або сайти не уразливі, або не можна фізично перехопити трафік - у зловмисника нічого не вийде. Однак, наявність одночасно і великої кількості пристроїв, і величезної кількості сайтів (приблизно на 36.7% із загальної маси сайтів і на 9.7% з мільйона найбільших сайтів) робить FREAK однією з найбільш небезпечних атак з усіх, що були виявлені за останній час. Що до перехоплення трафіку - багато людей користуються безкоштовним Wi-Fi і поняття не мають, як їм захистити свої домашні мережі.

МОЖЛИВІ ЗБИТКИ

Атака дозволяє зловмисникам відносно легко отримувати логіни і паролі від сайтів, інформацію з Інтернет-банків, зміст поштових повідомлень і так

далі. Вони можуть отримати все, що ви відправляєте на / через сайти, які захищені HTTPS-з'єднанням.

ЯК ЗАХИСТИТИСЯ ВІД АТАКИ FREAK

На стороні клієнта вразливість зачіпає OpenSSL (виправлено в 0.9.8zd, 1.0.0p і 1.0.1k), браузер Safari і різноманітні вбудовані та мобільні системи, включаючи Google Android і Apple iOS. Що стосується серверів, то сканування мережі показало, що набір RSA_EXPORT підтримується приблизно на 36.7% із загальної маси сайтів і на 9.7% з мільйона найбільших сайтів. Для захисту сервера на базі Apache до параметрів директиви SSLCipherSuite слід додати "! EXPORT".

ВИСНОВКИ

У WEB – світі багато вразливостей, які можуть бути сховані на багато років, але одного дня вони заявляють про себе усьому світі та загрожують безпеці персональних даних мільйонів користувачів інтернет. Будьте обачливими та серйозно відноситься до вашой віртуальної безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стаття: портал DELFI (Електрон. ресурс) / Спосіб доступу: URL: http://rus.delfi.lv/news/daily/story/istoriya-dnya-vse-pro-freak-novuyu-katastroficheskuyu-bresh-v-ustrojstvah-apple-i-android.d?id=45648354.
2. Стаття: блог лабораторії Касперского (Електрон. ресурс) / Спосіб доступу: URL: http://blog.kaspersky.ru/chto-takoe-chelovek-poseredine/740/.
3. Доклад: форум (Електрон. ресурс) / Спосіб доступу: URL: http://provisionsecurity.ru/threads/674/

УДК 004.01

ОСНОВНІ ВІДМІННОСТІ ЗВОДА ЗНАНЬ В ОБЛАСТІ КЕРУВАННЯ, УПРАВЛІННЯ ТА КОНТРОЛЯ IT COBIT 5 ВІД COBIT 4.1

Шуман Дар'я Сергіївна[1], Тимофєєв Дмитро Сергійович
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail:sugar-bowl@mail.ru[1]

В статті розглядається CobiT 5 як новий стандарт для IT-функцій, організацій та постачальників послуг в галузі IT. В роботі розглянуті відмінності між CobiT 4.1 і CobiT 5, які дають змогу прослідкувати та оцінити еволюцію документу COBIT.

Ключові слова – система управління; система керівництва; сфера IT; інвестиції в інформацію.

ВСТУП

COBIT дозволяє підприємствам отримувати від інформації, що стала валютою 21-го сторіччя, максимальну кількість користі при мінімумі ризиків.

CobiT 5 – наступний еволюційний крок у визначенні підходів управління IT для підтримки бізнес-діяльності організації, щоб досягти саме таких стратегічних цілей, які потрібні для ефективного вирішення оперативних потреб. Сьогодні більш ніж коли-небудь інформація і відповідні технології повинні регулюватися, керуватися і працювати на основі комплексного підходу єдиної інтегрованої моделі процесу, що повністю забезпечує охоплення ролей, обов'язків та необхідну практику.

ВДОСКОНАЛЕННЯ CobiT

Значні поліпшення були внесені до методології CobiT, а саме - позиціонування його як моделі для корпоративного управління інформаційними технологіями. На відміну від своїх попередників CobiT 4.1 та ITIL v3 (англ. Information Technology Infrastructure Library, бібліотека інфраструктури інформаційних технологій), підходи CobiT 5 охоплюють всі три рівні в рамках управління IT.

CobiT 4.1 та ITIL v3 – це моделі процесу, які описують IT-практики організації підприємства на оперативному рівні та являються корисним ресурсом для продуктивного використання.

Проте ні CobiT 4.1, ні ITIL v3 не вирішують потреби ефективного керування та продуктивного використання IT-ресурсів. Також вони не описують процеси корпоративного управління, необхідні для керівництва і контролю використання IT.

Поліпшення CobiT5 включають реструктуризацію описів окремих процесів, визначення фактичних базових дій в рамках кожного процесу, і описання ключових заходів в межах кожної базової діяльності. [2]

Весь матеріал CobiT 5 будується на п'яти основних принципах, які фактично забезпечують мотив та можливість для різних практичних дій по керівництву по управлінню IT:

1. Відповідність вимогам та очікуванням зацікавлених сторін;
2. Комплексний погляд на підприємство;
3. Застосовування єдиної інтегрованої методики;
4. Забезпечення цілісності підходу;
5. Розподіл управління та керівництва.

Найбільш суттєва зміна в CobiT – реорганізація:

- Структури від моделі IT-процесів до підходів керівництва IT з набором практик управління в цій області;

- Системи управління для безперервного вдосконалення діяльності у галузі IT;
- Моделі процесу з вихідним досвідом.

Різниця між системою управління та системою керівництва добре окреслена. (Рис.1)

Керівництво гарантує, що цілі підприємства досягаються шляхом оцінки суб'єктів діяльності, умов і опцій; встановлення напрямку шляхом прийняття рішень та вибору пріоритетів; моніторингу продуктивності, дотримання та покращення узгоджених керівництвом цілей та настанов.

Управління планує, будує, працює і контролює діяльність у відповідності з директивами, які задані органом управління для досягнення цілей підприємства.

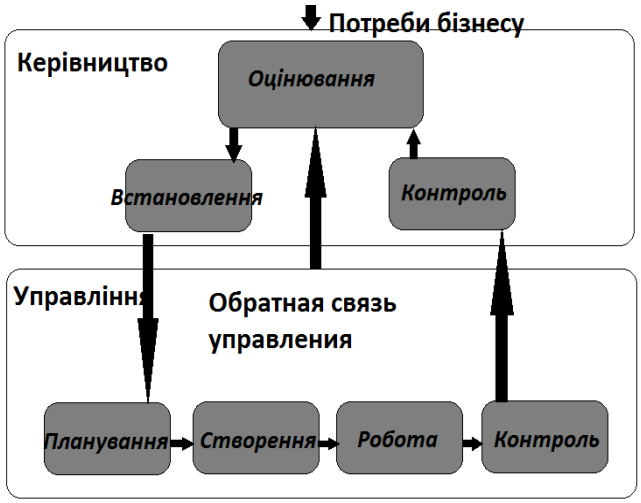


Рисунок1. Система управління та система керівництва

CobiT 5 надає нові процеси управління, які покращують підходи до управління, що були залучені у CobiT 4.1, Val IT (англ..Getting best value from IT investments, набір практик управління IT-процесами, націлених на збільшення прибутків від IT-інвестицій) та Risk IT (набір практик з будування системи управління IT-ризиком.

Це керівництво:

- Допомагає підприємствам уточнювати і зміцнювати високий рівень менеджменту відповідно до GEIT (англ. Governance of Enterprise IT, управління підприємством IT);
- Підтримує інтеграцію GEIT в існуючу практику управління підприємством у відповідність із ISO / IEC 38500.

CobiT 5 пояснює рівні процесів управління та інтегрує CobiT 4.1, Val IT та Risk IT контент в одну еталонну модель. (Рис.2)

Для ефективного керівництва та управління IT самих тільки принципів недостатньо, тому потрібні і інші компоненти-фактори впливу. Їх сім:

1. Політики, принципи та підходи;
2. Процеси;
3. Оргструктура;
4. Культура, етика, поведінка;
5. Інформація;
6. Послуги, інфраструктура та додатки;
7. Люди, навики та компетенції.

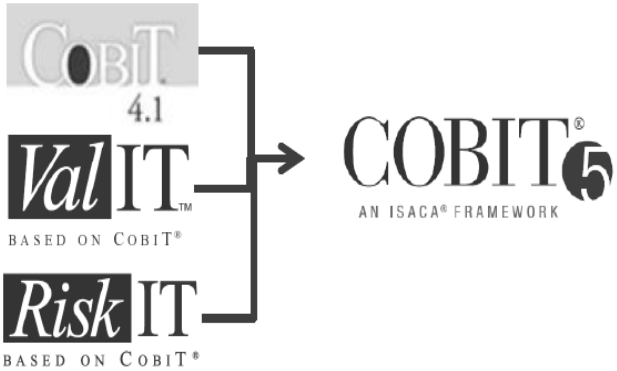


Рисунок 2. Інтеграція CobiT 4.1, Val IT та Risk IT

Є кілька нових і змінених процесів, які відображають сучасне мислення, зокрема:

- APO03 Управління архітектурою підприємства;
- APO04 Інноваційне управління;
- APO05 Управління портфелем;
- APO06 Управління бюджетом і витратами;
- APO08 Управління відносинами;
- APO13 Управління безпекою;
- BAI05 Управління змінами організаційними забезпечення;
- BAI08 Управління знаннями;
- BAI09 Управління активами;
- DSS05 Управління службою безпеки;
- DSS06 Управління контролю бізнес-процесів. [1]

РЕАЛІЗАЦІЯ CobiT 5

CobiT 5 включає операційну модель та просту спільну мову для всіх видів бізнесу, які мають діяльність в галузі IT.

Він також забезпечує основу для вимірювання і контролю продуктивності IT, інтегруючи кращі практики управління, менеджменту та зв'язку з зацікавленими сторонами.

Підходи CobiT 5 включають базову модель процесу, визначають і описують процеси управління та менеджменту. Еталонна модель процесу включає в собі всі процеси, які зазвичай перебувають на підприємствах, пов'язаних з IT-діяльністю, надаючи загальну модель, яка зрозуміла працівникам IT-сфери та менеджерам компаній.

Модель процесу CobiT 5 – це повна, всебічна модель, яку підприємство повинно адаптувати саме до своїх специфічних потреб, взявши до уваги внутрішні потреби бізнесу, зовнішній тиск, виконання підприємством своїх функцій, які відповідають вимогам зацікавлених сторін організації.

Реалізація CobiT 5 починається з визначення того, які інтереси зацікавлених сторін будуть мати пріоритет, які їхні очікування, чи матимуть відповідні можливості IT-функції, щоб задовольнити ці очікування і хто буде нести відповідальність за це.

Це вимагає знань про основні процеси і систему менеджменту, які підтримує IT-функції надання послуг та очікувану продуктивність.[2]

ВИСНОВКИ

COBIT 5 являє собою всеоб'ємлючу структуру загальноприйнятих принципів, практик, аналітичних

інструментів і моделей, які можуть допомогти будь-якому підприємству ефективно вирішувати найважливіші питання бізнесу, пов'язані з керуванням і управлінням інформацією і технологіями.

COBIT 5 об’єднує п’ять основних принципів, які дозволяють підприємству на основі семи факторів впливу організувати ефективне керівництво та управління, які дають змогу оптимізувати інвестиції в інформацію і технології, забезпечити їх успішне використання на благо зацікавлених осіб.

Вдосконалена версія CobiT 5 - це не просто покращення популярного підходу, це майже повністю новий продукт з іншою сферою, іншою аудиторією, іншою структурою та претензією на нову, більш важливу роль в системі знань управління корпоративними IT.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISACA — международная ассоциация, объединяющая профессионалов в области ИТ (Електрон.ресурс) / Спосіб доступу: URL: http://www.isaca.org.

2. QAP (qualified advice partner) (Електрон.ресурс) / Спосіб доступу: URL: http://www.qualified-audit-partners.be.

Секція «Інформаційно-вимірювальні технології»

Голова секції: д.т.н., професор кафедри метрології та інформаційно-вимірювальних технологій Корсун В.І.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Мілінчук Ю.А.

УДК 681.518.3

ПРИМЕНЕНИЕ СРЕДЫ LABVIEW ДЛЯ ИССЛЕДОВАНИЯ ПРОЦЕССА ПЕРЕРАСПРЕДЕЛЕНИЯ ЗАПАСЕННОЙ ЭНЕРГИИ В ЕМКОСТНЫХ ДАТЧИКАХ

Харламова Юлия Николаевна[1], Корсун Валерий Иванович
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://mivt.nmu.org.ua, E-mail: harlamyshka@yandex.ua[1]

Рассмотрены вопросы влияния изменения параметров электрической цепи на процесс перераспределения запасенной энергии. Представлен виртуальный лабораторный стенд для исследования переходных процессов.

Ключевые слова – перераспределение запасенной энергии; емкостные датчики; емкостные влагомеры; переходный процесс.

ВВЕДЕНИЕ

Емкостные датчики – преобразователи параметрического типа, в которых изменения измеряемой величины трансформируется в изменение емкостного сопротивления. Емкостные датчики нашли широкое применение в разных отраслях промышленности для измерения давления, деформации, толщины диэлектрических материалов, линейных и угловых ускорений, влажности и др.

Емкостные влагомеры основаны на электрическом методе определения содержания влаги в древесине и используют отношения между содержанием влаги и измеряемых диэлектрических свойств древесины (диэлектрическая проницаемость, коэффициент диэлектрических потерь или сочетания того и другого).

Диэлькометрический метод измерения влажности осуществляется с применением влагомеров, состоящих из емкостных датчиков и измерительных блоков, преобразующих изменения электрической емкости датчика, вызываемые изменением влажности древесины, в выходной сигнал [1].

Рассмотрим влагомер, в котором в качестве датчика используется параллельно соединенный резистор R с последовательно соединенным конденсатором C с резистором r. Изменение напряжения U_C на конденсаторе от времени t описывается уравнением:

$$U_C(t) = E \cdot (1 - e^{\frac{-t}{(C \cdot r)}}), \qquad (1)$$

где t – время переходного процесса (с); E – напряжение (В).

Рассмотрим площадь S_1, ограниченную линией установившегося состояния E_0 и кривой $U_C(t)$, которая пропорциональна энергии, запасенной в объекте управления (рис. 1).

$$S_1 = E \cdot \int_0^{\infty} (1 - e^{\frac{-t}{(C \cdot r)}}) dt = E \cdot \int_0^{\infty} e^{\frac{-t}{(C \cdot r)}} dt = E \cdot C \cdot r$$

Если увеличить управляющее воздействие до значения E_{max}, то координата E должна принять установившееся значение $E_{\max}$ при том же характере изменения $U_C(t)$ [2].

Для определения площади S_2, ограниченной кривой $U_C(t)$ до значения E_0, найдем из (1) время t_2:

$$t_2 = C \cdot r \cdot \ln \frac{E_{\max}}{E_{\max} - E_0}$$

Тогда площадь S_2 выражается формулой:

$$S_2 = E \cdot \int_0^{t_2} e^{\frac{-t}{(C \cdot r)}} dt = E \cdot C \cdot r \cdot (1 - e^{\frac{-t}{(C \cdot r)}}) =$$

$$= E \cdot C \cdot r \cdot (1 - e^{-\ln \frac{E_{\max}}{E_{\max} - E_0}}) = E \cdot C \cdot r$$

Таким образом, площадь S_2 равна площади S_1. Из этого следует, что энергия, запасенная в объекте к моменту времени t_2, равна энергии, соответствующей значению E_0. Чтобы удерживать координату на значении E_0 необходимо в момент времени t_2 сделать переключение управляющего воздействия от значения E_{max} до значения E_0 и поддерживать управление на уровне E_0.

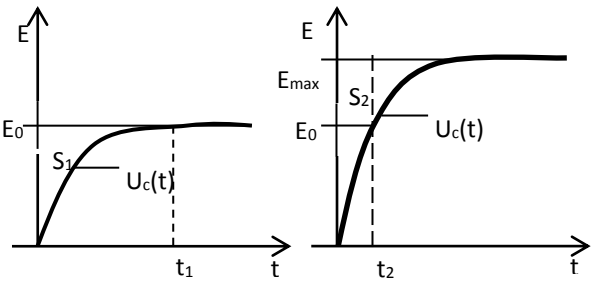


Рисунок 1. Кривые напряжения на конденсаторе

МЕТОДИКА ИССЛЕДОВАНИЯ

Для исследования переходного процесса, описываемого уравнением (1), был разработан виртуальный лабораторный стенд (рис. 2) с использованием среды графического программирования LabView [3]. Представленный лабораторный стенд наглядно иллюстрирует изменение напряжения на конденсаторе в зависимости от времени и влияние изменения управляющего воздействия на процесс перераспределения энергии.

Значения напряжения E_0 и E_{max}, электрической емкости C и сопротивления r, для дальнейших расчетов, вводятся через регуляторы типа Numeric Control. Индикатор типа Progress Bar служит для иллюстрации скорости протекания переходного процесса. На индикаторы типа Numeric Indicator выводятся значения: напряжения на конденсаторе U_C и U_{C2} при заданных значениях E_0 и E_{max} соответственно; значения площади S_1 и S_2; время переходного процесса t_1 (при управляющем воздействии E_0) и t_2 (при управляющем воздействии E_{max}).

На графике *а* (рис. 2) изображена кривая изменения напряжения U_C от времени t, при управляющем воздействии E_0 (рис. 2, в). На графике *б* (рис. 2) изображено изменение напряжения U_{Cmax} от времени t, при управляющем воздействии E_{max}.

В момент времени t_2 происходит переключение управляющего воздействия от значения E_{max} до значения E_0 (рис. 2, г), напряжение U_{C2} сразу принимает установившееся значение U_C, равное E_0, что изображено на рис. 2, б. По истечению времени t_2 управление поддерживается на уровне E_0.

РЕЗУЛЬТАТЫ

Моделирование управления переходным процессом позволяет сделать следующие выводы:

1. Подведенная энергия расходуется на изменение запаса внутренней энергии и на полезную работу, при отключении – запасенная энергия превращается в полезную работу, вызывая изменения напряжения U_C.

2. При любом максимальном управляющем воздействии E_{max} энергия, запасенная к моменту времени t_2, равна энергии, соответствующей любому значению E_0.

3. Для оптимального управления (для достижения E_0 за минимальное время длительностью t_2) требуется максимальное значение воздействия E_{max}. После достижения заданного значения управление должно поддерживаться на уровне E_0.

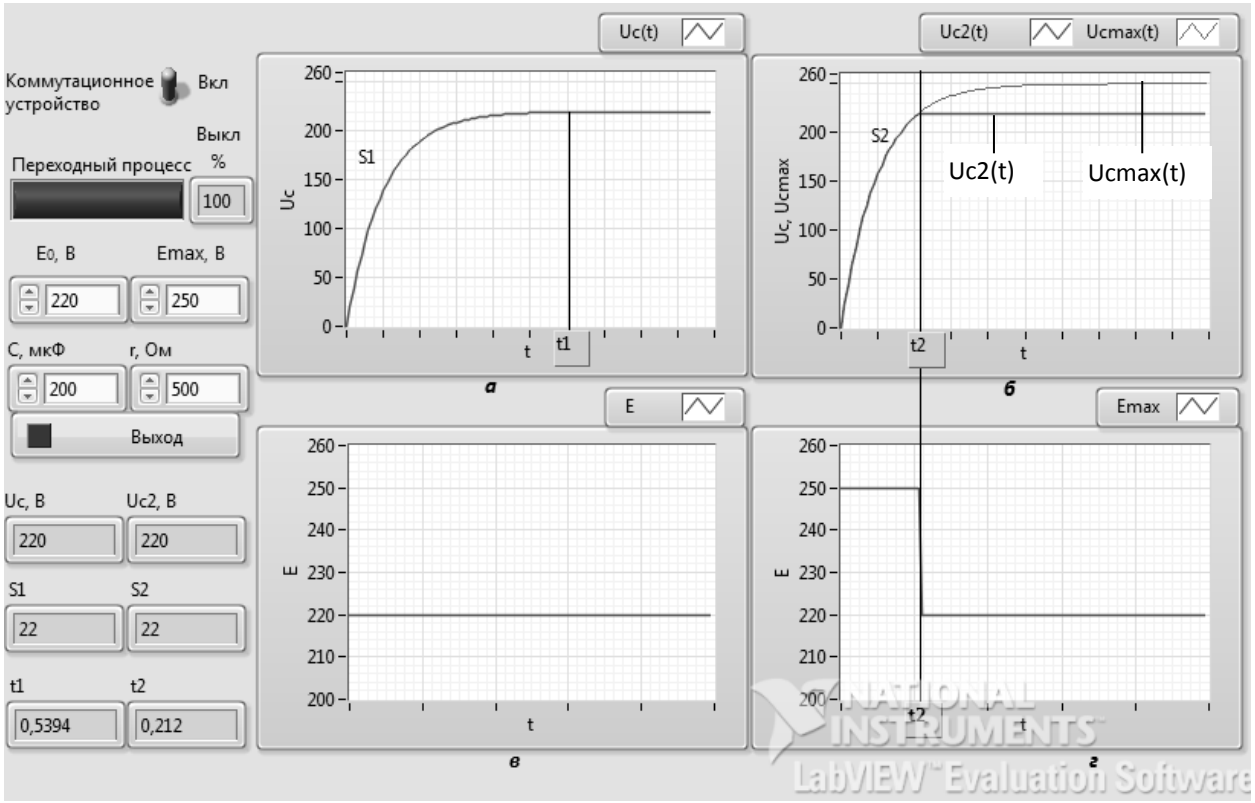


Рисунок 2. Виртуальный лабораторный стенд для исследования управления переходным процессом

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Харламова Ю.Н. Анализ методов контроля влажности древесины / Ю.Н. Харламова // Молодежь: наука и инновации: Вторая всеукр. научн.-техн. конф. студентов, аспирантов и молодых ученых (02-03 декаб 2014 г., Днепропетровск) : / тезисы докладов / М-во образования и науки Украины, Национальный горный университет. – Д., 2014. – Том 12. – С 44-45.

2. Олейников В.А. Основы оптимального и экстремального управления. / В.А. Олейников, Н.С. Зотов, А.М. Пришвин. – М.: «Высшая школа», 1969. – 296 с.

3. Глухова Н.В. Метрологія динамічних вимірювань. Частина ІІ. Моделювання та вимірювання параметрів динамічних процесів в електричних колах. Методичні вказівки до лабораторних робіт для студентів напряму підготовки 8(7).05100101 «Метрологія та вимірювальна техніка» / Н.В. Глухова, Ю.М. Харламова. – Д.: Національний гірничий університет, 2015. – 56 с.

УДК 621.311:537

МОДЕЛІ ТИПОВИХ ЗБУРЕНЬ ХВИЛЬОВОЇ СТРУКТУРИ

Дороніна Марина Анатоліївна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://mivt.nmu.org.ua, E-mail: doroninam@nmu.org.ua

Наведенні моделі типових збурень хвильової структури, які використовуються в теорії регуляторів, що пристосуються до збурень.

Ключові слова: динамічна система, збурення хвильової структури.

ВСТУП

З розвитком сучасних інформаційно-вимірювальних технологій та засобів обробки інформації постійно зростають вимоги до забезпечення точності. У зв'язку з цим актуальною є задача протидії реальним впливам динамічного характеру, які призводять до небажаних ефектів на виході системи, особливо в складних многомірних системах. Збурення можна поділити типу шум та хвильової структури. Збурення типу шум мають хаотичний характер, якому не властива регулярність. Його результативно можна оцінити за допомогою методів статистичного аналізу [1, 2]. Збурення хвильової структури мають хвильоподібні форми, хоча б на певних ділянках часу. Такі збурення можуть мати лінійний, ступінчатий або хвильовий характер. Для оцінки таких збурень доцільно використовувати «теорію регуляторів, що пристосовуються до збурень» [3. 4]. Ця теорія вважається універсальним методом для вирішення задач оцінки збурень хвильової структури.

ХВИЛЬОВЕ ПРЕДСТАВЛЕННЯ ЗБУРЕНЬ

Збурення хвильової структури можна представити у вигляді напівдетермінованих аналітичних виразів:

$$\omega(t) = c_1 f_1(t) + c_2 f_2(t) + \dots c_n f_n(t) \qquad (1)$$

де $c_1 \cdots c_n$ - це кусково-постійні вагові коефіцієнти.

Тобто згідно з (1) $\omega(t)$ може бути представлений у момент часу t у вигляді певної зваженої комбінацією відомих базисних функцій $f_1(t) \dots f_n(t)$ [2].

Припустимо, що для кожної базисної функції існує перетворення по Лапласу $f_1(s) \dots f_n(s)$.

Рівняння (1) можна представити у вигляді:

$$\omega(s) = c_1 f_1(s) + c_2 f_2(s) + \dots c_n f_n(s) = \sum_{i=1}^{n} c_i \frac{P(s)}{Q(s)}, \qquad (2)$$

де $Q(s)$ є найменшим загальним знаменником серед множини інших знаменників у перетвореннях за Лапласом базисних функцій, а $P(s)$ несе в собі інформацію про початкові умови та стрибкоподібні коефіцієнти $c_1 \dots c_m$.

Тоді $\omega(t)$ можна розглядати, як вихідну змінну фіктивної лінійної динамічної системи.

$$\omega(s) == \frac{1}{Q(s)} P(s) \qquad (3)$$

Загальний знаменник $Q(s)$ можна представити у вигляді:

$$Q(s) = s^k + a_k s^{k-1} + a_{k-1} s^{k-2} + \dots + a_1 \qquad (4)$$

Тоді враховуючи рівняння (3) та (4) збурення $\omega(t)$ перепишемо у вигляді лінійного диференціального рівнянню:

$$\frac{d^k \omega}{dt^k} + a_k \frac{d^{k-1} \omega}{dt^{k-1}} + a_{k-1} \frac{d^{k-2} \omega}{dt^{k-2}} + \dots + a_1 \omega = 0 \qquad (5)$$

де $a_1 \dots a_k$ - відомі коефіцієнти.

Для того щоб врахувати стрибкоподібні зміни коефіцієнтів $c_1 \dots c_n$ в роботі [3] пропонується ввести послідовність функцій Дірака, що будуть грати роль зовнішньої довільної змушуючої сили.

$$\frac{d^k \omega}{dt^k} + a_k \frac{d^{k-1} \omega}{dt^{k-1}} + a_{k-1} \frac{d^{k-2} \omega}{dt^{k-2}} + \dots + a_1 \omega = \delta(t) \qquad (6)$$

У зв'язку з введення зовнішнього збурюючого сигналу $\delta(t)$ на вході системи, модель немов би оновлюється і буде працювати з новими початковими умовами.

МОДЕЛІ СТАНУ ТИПОВИХ ЗБУРЕНЬ ХВИЛЬОВОЇ СТРУКТУРИ

Розглянемо типові збурення хвильової структури. Зокрема, проаналізуємо збурення, які можна описати лінійною комбінацією (рис.1). Такі збурення можна представити аналітичним виразом: $\omega(t) = c_1 + c_2 t$

Згідно з рівнянням (6) модель збурення буде мати вигляд:

$$\frac{d^2 \omega}{dt^2} = \delta(t) \qquad (7)$$

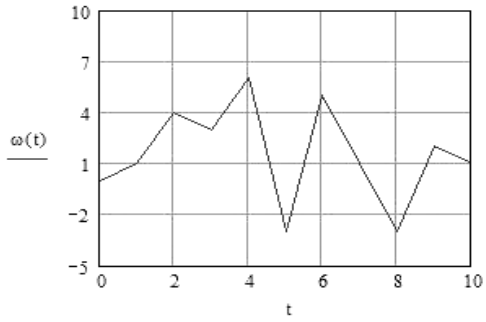


Рис.1.Збурення. що описуються лінійною комбінацією

Збурення хвильової структури, які мають ступеневий характер (рис.2) можна описати виразом: $\omega(t) = c$. Тоді модель зміни станів буде:

$$\frac{d\omega}{dt} = \delta(t) \tag{8}$$

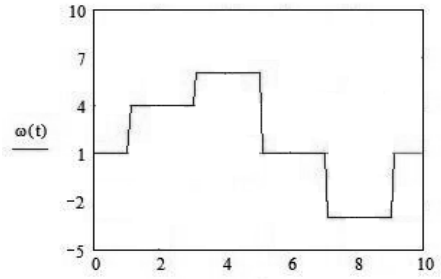


Рис.2. Збурення, що описуються ступінчатою функцією

Збурень, що мають експоненціальний характер (рис. 3) можна описати, як $\omega(t) = c_1 + c_2 e^{-\beta t}$. Тоді модель зміни часу матиме вигляд:

$$\frac{d^2\omega}{dt^2} + \beta\frac{d\omega}{dt} = \delta(t) \tag{9}$$

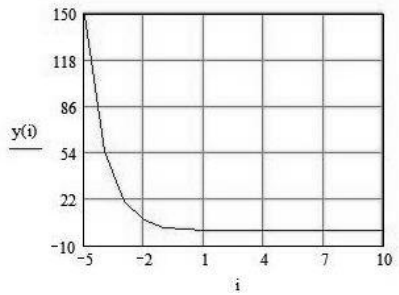


Рис.3. Збурення, що описуються експоненціальною функцією

Доволі розповсюджені збурення, що мають синусоїдальний характер, такі збурення можна аналітично описати $\omega(t) = c_1 + c_2 \sin \alpha t$. Відповідно модель збурення буде:

$$\frac{d^2\omega}{dt^2} + \alpha\frac{d\omega}{dt} = \delta(t) \tag{10}$$

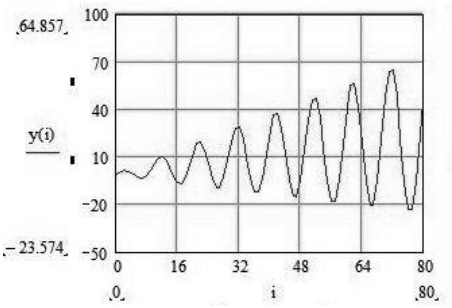


Рис.4. Збурення, що описуються синусоїдальною функцією.

Ще один розповсюджений випадок, це використання згасаючої синусоїди як базисної функції $\omega(t) = c_1 + c_2 e^{-\gamma t} \sin \alpha t$ Тоді модель змінн такої функції буде складати:

$$\frac{d^3\omega}{dt} + 2\gamma\frac{d^2\omega}{dt^2} + (\gamma^2 + \alpha^2)\frac{d\omega}{dt} = \delta(t) \tag{11}$$

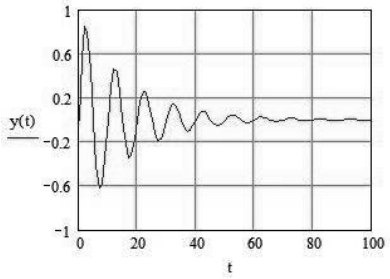


Рис.5. Збурення, що представлені за допомогою згасаючої синусоїдальної функції

Представлені моделі стану типових збурень хвильової структури можна використовувати як окремі базисні функції, але й комбінувати для опису складних многомірних динамічних процесів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Егупов Н.Д. Методы классической и современной теории автоматического управления. Учебник. Том 1. / Н.Д. Егупов, К.А. Пупков. М.: МГТУ им. Н.Э.Баумана, 2004, - 748 с.

2. Василенко Г.И. Теория восстановления сигналов. / Г.И. Василенко. М.: Советское радио. 1979. – 270 с.

3. Джонсон С. Теория регуляторов, приспосабливающихся к возмущениям./С. Джонсон; пер. с англ. // Фильтрация и стохастическое управление в динамике систем. – М.: Мир, 1980.-487 с.

4. Андреев Ю.П. Управление конечномерными линейными объектами./Ю.Н. Андреев. М.: Наука, 1976. - 424 с.

Голова секції: к.т.н., доцент кафедри програмного забезпечення комп'ютерних систем Удовик І.М.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Гуліна І.Г.

УДК 681.515: 519.7: 62-52

АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОЦЕССАМИ ДРОБЛЕНИЯ И ИЗМЕЛЬЧЕНИЯ РУД

Мацюк Сергей Михайлович
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://pzks.nmu.org.ua, E-mail: matsuk_sergei@mail.ru

В работе рассмотрены автоматизированные системы управления технологическими процессами дробления и измельчения, проанализированы их достоинства и недостатки.

Ключевые слова – объект управления, автоматизированные системы управления, технологический процесс, интерфейс системы.

ВВЕДЕНИЕ

Рудоподготовка включает процессы дробления и измельчения, затраты на которые составляют больше половины себестоимости горно-обогатительного производства. Поэтому актуальной задачей является проведение исследований для снижения затрат по этим процессам путем создания информационных систем автоматизированного управления.

ОСНОВНАЯ ЧАСТЬ

В работе [1] предложена система автоматической оптимизации процесса крупнокускового дробления, которая включает датчики контроля ширины разгрузочной щели дробилки ККД-1500/180, а также крупности и прочности ее входной руды. Целью управления является оптимизация содержания класса +100 мм в дробленой руде, который контролируется с помощью поточного гранулометра.

Оптимизация управления шириной разгрузочной щели осуществляется на основе прогнозирующей модели процесса в виде конечно-разностного уравнения, параметры которого могут адаптироваться в ходе работы системы.

Недостатком этой системы является невысокая точность, обусловленная погрешностями используемой модели и датчиков контроля.

Примером комплексного подхода к решению задачи оптимального управления технологическим процессом дробления является (АСУ) дробилками КМД-3000Т2ДДП и КСД-2200Т2-Д, реализованная на базе микропроцессорных средств фирмы «Siemens» и внедренная на СП «Ерденет» (Монголия) [2] (рис. 1).

Недостатком этой АСУ является ее неинвариантность к целям управления. Например, невозможно с ее помощью организовать управление гранулометрическим составом продукта дробления.

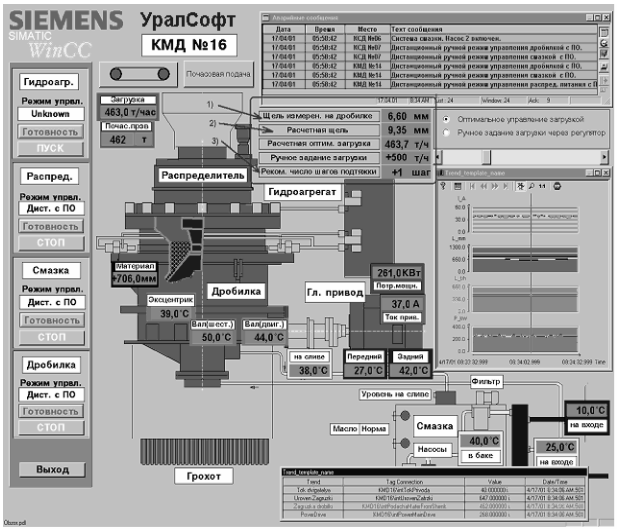


Рисунок 1. Интерфейс АСУ дробилки

Наиболее эффективными являются адаптивные системы, основанные на структурных моделях объекта управления (ОУ) с параметрической идентификацией в процессе управления. Такие системы характеризуются сложными алгоритмами обработки информации в управляющей части и появились благодаря развитию современных средств вычислительной техники.

К недостаткам этих систем относят использование линейных моделей для прогноза нелинейных процессов измельчения, а также неоптимальность управления. Однако, использование оперативных данных о внутреннем состоянии объекта и априорной информации о закономерностях измельчения в сочетании с современными методами адаптивной идентификации и управления, является наиболее перспективным методом, базирующемся на контроле переменных состояния ОУ [3].

Примером адаптивной системы является автоматизированная система управления технологическим процессом (АСУ ТП) рудоподготовки MineOOcad компании National Steel Pellet Company (США, штат Миннесота) [4]. Данная система выполняет процедуры идентификации и

прогнозирования процессов дробления и измельчения (рис. 2).

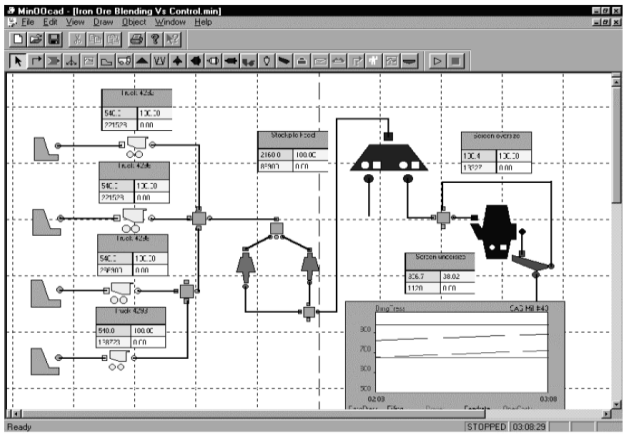


Рисунок 2. Интерфейс АСУ MineOOcad

Внедрение данной системы позволило увеличить производительность за счет улучшения измельчения руды на 15% и уменьшить время разгрузки грузовиков на 25%, а также уменьшить складские запасы.

К достоинствам системы также следует отнести: сокращение расходов электроэнергии и других ресурсов; система работает с любым числом элементов технологического процесса; полученные модели достаточно точно аппроксимируют все элементы технологических процессов дробления и измельчения руд.

Примером автоматизации линии магнитного обогащения железных руд является АСУ ТП рудообогатительной фабрики №1 (РОФ-1) на Ингулецком ГОК (рис. 3), в которой реализованы локальные системы автоматического регулирования.

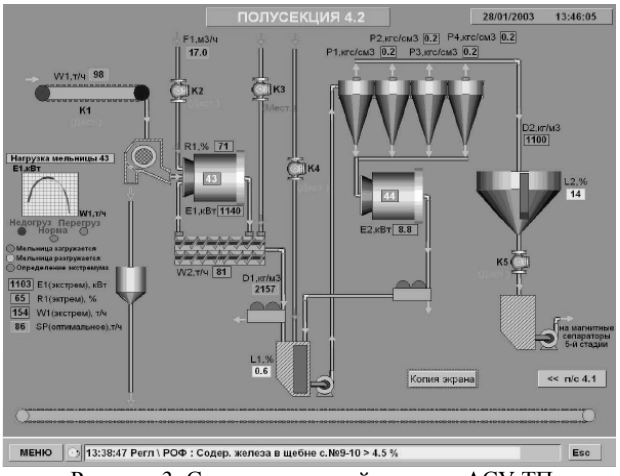


Рисунок 3. Структура первой очереди АСУ ТП секции обогащения

К недостаткам этой АСУ ТП следует отнести реализацию только статической оптимизации процессом измельчения, который приводит к потерям в динамических (переходных) режимах.

Ключевые элементы, требуемые для этих АСУ – адекватные модели, точные процедуры оценки, основанные на измерениях, а также недорогие аппаратные средства управления для реализации функций стабилизации и оптимизации.

Примером реализации в Украине адаптивной системы является АСУ ТП секций обогащения руды, реализованной ОАО «Северный ГОК» и разработанной на базе SCADA-системы TRACE MODE 6 [5].

Недостатком данной АСУ ТП является неэффективность реализации линейных законов регулирования нелинейным нестационарным процессом измельчения.

ВЫВОДЫ

В результате проведённых исследований установлено, что существующие информационные системы управления процессами дробления и измельчения руд имеют следующие недостатки: неинвариантность к целям управления; использование линейных моделей для прогноза нелинейных процессов дробления и измельчения, а также не оптимальности управления.

Дальнейшие исследования должны бать направлены на разработку информационных систем управления дроблением и измельчением руд, реализующих оптимальное управление процессами с их интеллектуальным прогнозированием.

ПЕРЕЧЕНЬ ИСТОЧНИКОВ

1. Качан Ю.Г. Вычислительные исследования алгоритма оптимизации процесса крупнокускового дробления / Ю.Г. Качан, В.И. Корниенко // Горн. электромеханика и автоматика: Респ. межвед. науч.-техн. сб. – 1988. – Вып. 53. – С. 48-53.

2. Богданчиков В.М. Автоматизированная система управления дробилкой (агрегированная АСУ) / В.М. Богданчиков, С.П. Цедилкин. – http:// www.ural-soft.com.ru.

3. Herbst J. A. Modern Control Theory Applied to Crushing. Part 1 : Development of a Dynamic Model for a Cone Crusher and Optimal Estimation of Crusher Operating Variables / J. A. Herbst, A. E. Oblad // Proc. of the 1st IFAC Symposium on Automation for Mineral Resource Development. - Pergamon Press, Oxford, 1986. – P. 301-307.

4. Herbst J.A. Model-based control of mineral processing operations / J.A. Herbst, W.T. Pate, A.E. Oblad // Powder Technology. – 1992. – Vol. 69. P. 21-32. – ISSN 0032-5910.

5. SCADA TRACE MODE в АСУТП обогащения руды Северного ГОКа. – http://www.tracemode.ua.

УДК 004.021

ПРОГРАМНО-МАТЕМАТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОБЧИСЛЕННЯ РОЗРІДЖЕНИХ МАТРИЦЬ

Мінько Олег Володимирович[1]
Науковий керівник: доц., к.ф.-м.н., Бердник М.Г.
Дніпропетровський національний університет ім. Олеся Гончара, м. Дніпропетровськ, Україна,
http://dnu.dp.ua, E-mail: minko.oleg@gmail.com[1], mgb2006@ukr.net

В роботі розроблено програмно-математичне забезпечення для роботи з розрідженими матрицями за допомогою технології Open MP.

Ключові слова – розріджені матриці, формат crs, операції над розрідженими матрицями, паралельна реалізація, орептр.

ВСТУП

Ефективні методи зберігання та обробки розріджених матриць протягом останніх десятиліть викликають інтерес у широкого кола дослідників [1-4]. Робота присвячена обчисленню розріджених матриць, що здійснюється за допомогою алгоритмів обробки матриць. В ході роботи були розроблені блок-схеми та програмне забезпечення для роботи з розрідженими матрицями для наступних операцій:

- транспонування;
- множення розріджених матриць;
- множення розрідженої матриці на щільний вектор;
- додавання розріджених матриць.

Відповідно до структури збереження розріджених матриць було реалізовано оптимізовані алгоритми обробки матриць. Для прискорення роботи програми була використана технологія OpenMP, яка дозволила розпаралелити наступні алгоритми:

- множення розріджених матриць;
- множення розрідженої матриці на щільний вектор.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Провівши експерименти використовуючи для обчислення матриці різного порядку та порівнюючи час виконання роботи програми на 1 потоці, на 8 потоках та за допомогою бібліотеки MKL. Результати експерименту наведені на рис. 1. та рис. 2.

Проаналізувавши отримані результати приходимо до висновку, що наша реалізація працює повільніше для матриць, порядок яких менший 20000, а переходячи цей порядок іде виграш у часі для 8 потоків.

Обчислювальні експерименти проводилися з використанням наступних інфраструктур, характеристики яких наведені у табл. 1. та табл. 2

Таблиця 1. Тестова інфраструктура №1

Процесор	Intel(K) core(TM) i7-3632QM CPU @ 2.20Ghz
Пам'ять	8 Gb
Програмне середовище	Visual Studio Premium 2012
Операційна система	Windows 8 x64

Результати роботи програми на тестовій інфраструктурі №1

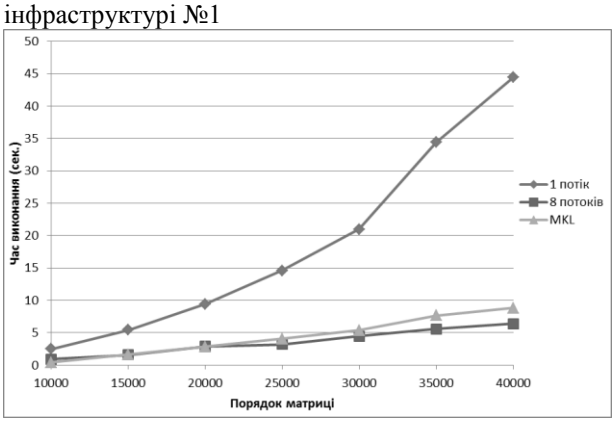


Рис. 1. Порівняння часу множення розріджених матриць (інфраструктура №1)

Таблиця 2. Тестова інфраструктура №2

Процесор	Intel® Core™ i5-5250U Processor (3M Cache, up to 2.70 GHz)
Пам'ять	4 Gb
Програмне середовище	Visual Studio Premium 2012
Операційна система	Windows 8.1 x64

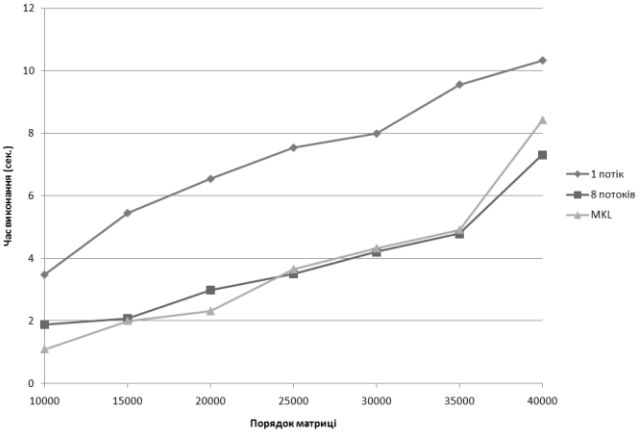


Рис. 2. Порівняння часу множення розріджених матриць (інфраструктура №1)

На рис. 3. показано час вирішення завдання за допомогою розроблених реалізацій з використанням різної кількості потоків:

- один потік;
- два потоки;
- чотири потоки;
- вісім потоків.

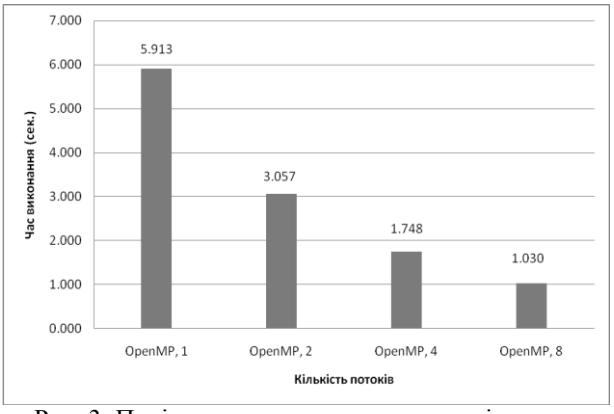


Рис. 3. Порівняння часу множення розріджених матриць на основі різної кількості потоків

ВИСНОВКИ

При аналізі результатів було помічено що спеціальні алгоритми обробки розріджених матриць працюють набагато швидше ніж їхні аналоги для обробки звичайних (щільних матриць) рис. 1. та рис. 2. чим більша розрідженість вхідних матриць тим ефективніше працюють реалізовані алгоритми. І навпаки, чим щільніша матриця, тим ефективніші будуть стандартні алгоритми її обробки. В загальному випадку слід враховувати структуру матриці перед тим, як використовувати той чи інший підхід для її обробки.

Отримані результати можуть бути використані при розв'язанні задач лінійної та нелінійної оптимізації, де вхідними параметрами є розріджені матриці. Ще однією із сфер застосування є чисельні реалізації методів математичної фізики, а саме при застосуванні:

- методу кінцевих елементів;
- методу сіток.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Писсанецки С. Технологія розріджених матриць. — М.: Мир,1988.
2. Джордж А., Лю Дж. Числове вирішення великих розріджених систем рівнянь. – М.: Мир, 1984.
3. Тьюарсон Р. Розріджені матрицы. – М.: Мир, 1977.
4. Паралельне і розподілене програмування з використанням C ++

УДК 004.51

ИНФОРМАЦИОННАЯ СИСТЕМА ОЦЕНКИ ВТОРИЧНОГО РЫНКА НЕДВИЖИМОСТИ НА ОСНОВЕ ПОСТРОЕНИЯ РЕГРЕССИОННЫХ МОДЕЛЕЙ

Гулин Алексей Алексеевич,
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://pzks.nmu.org.ua, E-mail: aagulin@rambler.ru

В работе разработан комплексный метод построения регрессионных моделей ценообразования на вторичном рынке недвижимости, позволяющий учитывать качественные факторы, обеспечивающий выявление и исключение мультиколлинеарных факторов.

Ключевые слова – колинеарность, коэффициент корреляции, выбросы, интерфейс системы.

ВВЕДЕНИЕ

Вторичный рынок недвижимости характеризуется наличием большого числа объектов недвижимости и жесткой конкуренции. В таких условиях решения об оценке объекта недвижимости должны приниматься на основе тщательного анализа имеющейся информации, быть мотивированными и обоснованными. Осуществляя мониторинг вторичного рынка недвижимости, приходится анализировать огромные объемы информации.

Информационная технология оценки объекта недвижимости, основанная на методах регрессионного анализа [1], позволяет наиболее точно определить стоимость объекта, охарактеризовать взаимосвязь и влияние на стоимость количественных и качественных факторов. [2].

ОСНОВНАЯ ЧАСТЬ

Предлагаемый комплексный метод построения регрессионных моделей оценки стоимости недвижимости включает в себя следующие этапы:

1. Обработка и предварительный анализ информации об объектах недвижимости с помощью описательной статистики, т.е. нахождение среднего, минимального и максимального значений, а также дисперсии и среднеквадратического отклонения для каждого количественного фактора.

2. Анализ матрицы парных коэффициентов корреляции между всеми факторами, с целью выявления факторов наиболее сильно влияющих на стоимость объектов недвижимости.

3. Выявление и устранение проблемы коллинеарности или мультиколлинеарности факторов. Для устранения проблемы коллинеарности или мультиколлинеарности факторов используется метод исключения ряда коррелированных переменных; в уравнении остаются факторы с минимальной величиной коэффициента множественной детерминации.

4. Построение полей корреляции (диаграммы рассеивания) зависимой и независимых переменных и на их основании установление формы связи переменными (рис.1).

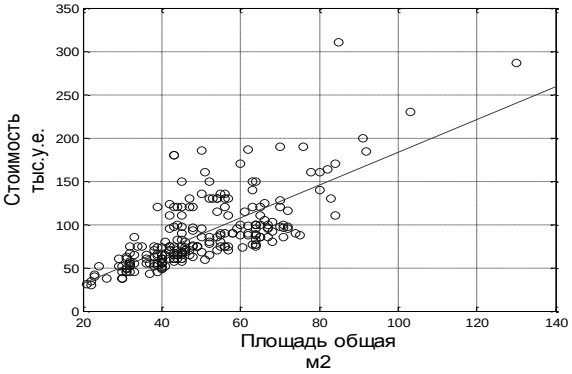


Рисунок 1. Пример построения полей корреляции

5. Поиск и удаление выбросов.

Выбросы – это нетипичные или редкие значения, которые существенно отклоняются от распределения остальных выборочных данных. Выбросы оказывают существенное влияние на угол наклона регрессионной линии и, соответственно, на коэффициент корреляции (рис.2).

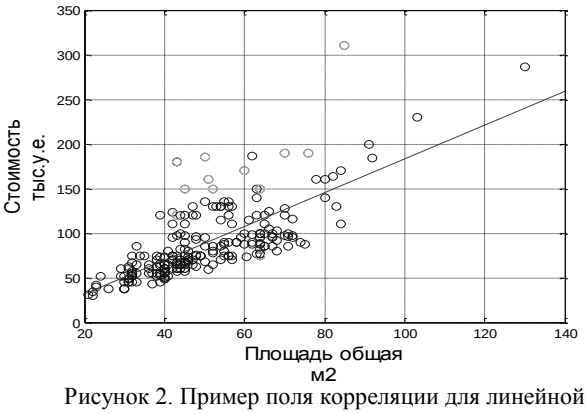


Рисунок 2. Пример поля корреляции для линейной регрессионной модели с отмеченными на них выбросами

Выбросы могут свидетельствовать о неоправданном завышении стоимости продаваемого объекта недвижимости, поэтому их необходимо исключать из рассмотрения.

Удаление выбросов осуществляется каждый раз перед построением регрессионной модели, включающей только количественные факторы.

Регрессионная модель, полученная в ходе исследования, позволяет получить наиболее точную и научно обоснованную оценку стоимости объекта недвижимости с учетом влияния на нее количественных и качественных факторов. В работе предложена информационная система, классы которой представлены на рисунке 3.

Входными данными для программы являются текстовые файлы с данными об объектах недвижимости.

Выходные данные могут быть подразделены на графические и числовые. К графическим выходным данным относятся: графики полей корреляции, векторная карта с обозначенными на ней объектами недвижимости. Числовыми выходными данными являются: описательные статистики количественных переменных, коэффициенты регрессионной модели, статистические показатели для оценки значимости, стоимость объекта недвижимости, полученная в окне оперативной оценки.

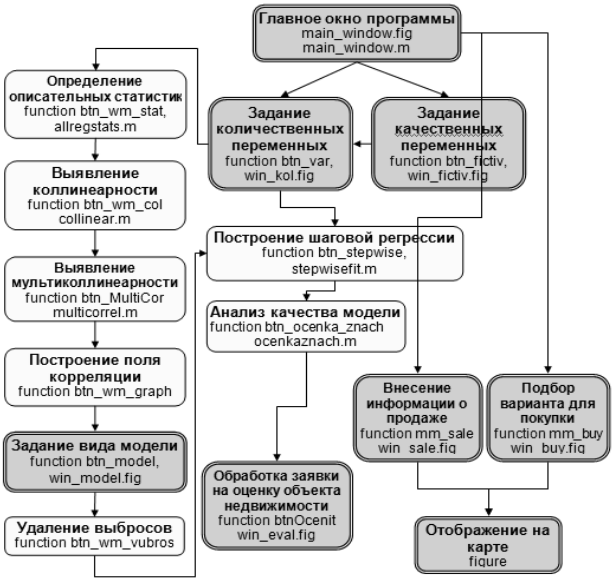


Рисунок 3. Перечень основных классов системы

На рисунке 4 представлено окно автоматической оценки стоимости объекта недвижимости на основе регрессионного анализа.

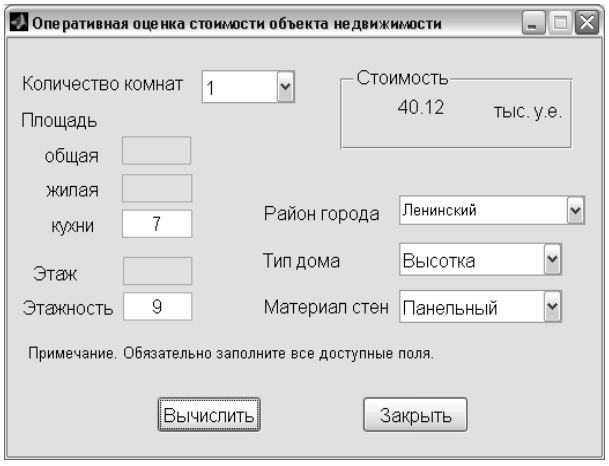


Рисунок 4. Интерфейс системы

Координаты объекта на карте автоматически считываются программой (рис. 5). Информация сохраняется в текстовый файл database.txt в виде строки с разделителем табуляции.

Практическое значение полученных результатов заключается в разработке программной реализации фрагмента ГИС мониторинга вторичного рынка недвижимости, позволяющей на основе разработанного метода производить оперативную обоснованную оценку объекта недвижимости и визуализацию его местоположения на векторной карте

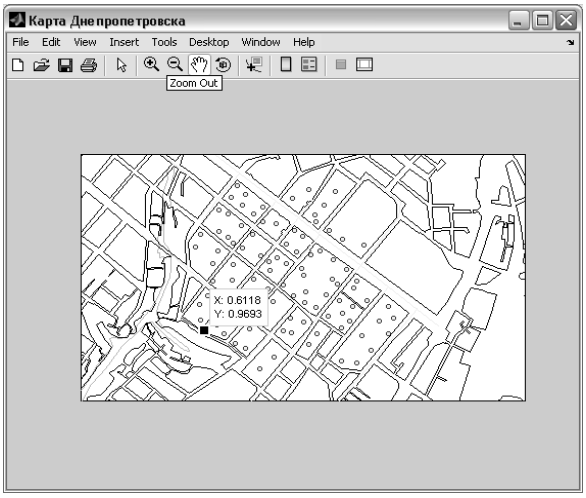


Рисунок 5. Определение объекта недвижимости на карте.

ВЫВОДЫ

В результате тестирования разработанного ПО проведен сравнительный анализ разных видов регрессионных моделей и, в конечном итоге, построена модель, дающая высокое качество оценки стоимости объектов вторичного рынка недвижимости, характерного для г. Днепропетровска.

Результаты работы могут использоваться для комплексного статистического анализа и принятия решений о стоимости объекта вторичного рынка недвижимости; для улучшения работы риэлтерских компаний. Регрессионная модель, полученная в ходе исследования, позволяет получить наиболее точную и научно обоснованную оценку стоимости объекта недвижимости с учетом влияния на нее количественных и качественных факторов.

ПЕРЕЧЕНЬ ИСТОЧНИКОВ

1. Себер Дж. Линейный регрессионный анализ. – М.: Мир, 1980. – 456 с.

2. Анализ вторичного рынка жилой недвижимости Днепропетровска. WEB-сайт / Способ доступа: URL: http://www.realnest.com.ua/information/articles/956

УДК 004

ИНФОРМАЦИОННАЯ СИСТЕМА ТЕХНИЧЕСКОГО АНАЛИЗА ФЬЮЧЕРСКИХ РЫНКОВ

Кумейко Оксана Сергеевна

Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua

В работе предложена информационная система для проведения технического и фундаментального анализа фьючерсных рынков (создан программный продукт, позволяющий проводить технический анализ данных, а именно: первичную обработку (фильтрация и сглаживание), осцилляторный и индикаторный анализ, аппроксимацию процесса Марковским с целью построения функций риска).

Ключевые слова – фильтрация, сглаживание, технический анализ данных, интерфейс системы.

ВВЕДЕНИЕ

Область применения продуктов, проводящих технический анализ очень большая: будь-то принятие решений на основе текущей деятельности фирмы, анализа кредитоспособности клиентов банка, оценка риска страховых операций, прогнозирование успеха биржевой деятельности или много других задач.

Этот современный уровень информационных технологий и задачи, связанные с такими продуктами, накладывают определенные требования на разработку автоматизированных рабочих мест оперативного анализа и прогнозирования фьючерсных рынков [1].

Современные программные средства должны предоставлять широкий спектр возможностей анализа для сведения потерь к минимуму, а так же сравнительных критериев используемых методов, чтобы помочь трейдеру определить оптимальный метод прогноза или мониторинга.

ОСНОВНАЯ ЧАСТЬ

Программный продукт «Forex Analyser» предназначен для технического анализа данных фьючерсных рынков в частности и также для анализа случайных процессов с изменяющимся трендом [2].

Поэтому входными данными для программы являются временные ряды, которые отображают развитие случайного процесса во времени (в частности ряды с котировками валют рынка Forex), содержащиеся в файлах специального формата [3].

Выходными данными являются: графическая информация – сглаженные временные ряды, точки разладки в процессе, которые обосабливают состояния процесса, индикаторы, осцилляторы и свечные фигуры, помогающие принять решение о состояниях рынка, график поведения смоделированного процесса; текстовая, числовая информация – вероятности пребывания рынка в том или ином состоянии, время, когда Марковский процесс, описывающий движение цен на рынке, входит в стационарный режим работы.

Для реализации каждой конкретной задачи были созданы отдельные модули и классы, представленные на рисунке 1.

Для написания продукта использовались такие среды: Microsoft Visual Studio 2007 (языке C# с использованием технологии .Net), Borland Delphi 7 (язык Object Pascal).

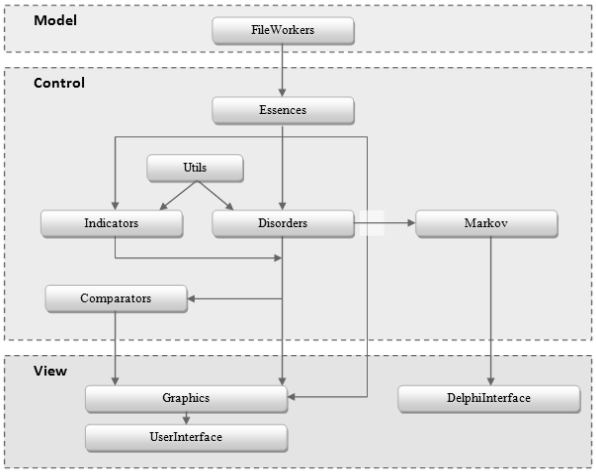


Рисунок 1. Модульная структура программы «Forex Analyser»

Рассмотрим содержимое некоторых пакетов и краткое описание файлов в них.

FileWorkers

- ReaderBarFromFile.cs – реализован интерфейс, описывающий общее поведение классов, загружающих данные с файла. Программа, таким образом, может работать с новыми типами файлов, которые необходимо прочесть;
- OrdinaryBarFile.cs – описан класс, читающий файлы, хранящие специальным образом данные фьючерсных рынков, а именно их пять составляющих: тиккер котировки, цену открытия, максимальную цену, минимальную цену, цену закрытия за каждый из периодов;
- OrdinaryBarFile.cs – описан класс, читающий файлы, хранящие одномерные временные ряды.

Essences

- Bar.cs – реализованы процедуры работы с данными фьючерсных рынков: ценой открытия, закрытия, максимальной и минимальной за отдельно взятые периоды;
- TimeRow.cs – реализован класс «Временной ряд». Содержит его поведение и свойства.

Indicators

- Indicator.cs – реализован абстрактный класс Indicator, содержащий описание поведения общего для всех индикаторов;
- Ind_<название индикатора>.cs – общее имя для всех файлов, в которых хранятся индикаторы.

Disorders

- DisorderMethod.cs – реализован абстрактный класс DisorderMethod, который содержит описание поведения общего для всех методов поиска разладок;
- DisorderMid.cs, DisorderDisp.cs, DisorderAngles.cs, DisorderCorridor.cs, DisorderMACD.cs – файлы, которые содержат классы, реализовывающие алгоритмы методов поиска разладок в случайном процессе.

Программа «Forex Analyser» имеет удобный, интуитивно понятный интерфейс, с удачным образом расположенными сворачивающимися панелями и информативными подсказками. Главное окно программы представлено на рисунке 2.

Самой главной отличительной способностью данного программного продукта является оценка точности работы осцилляторов.

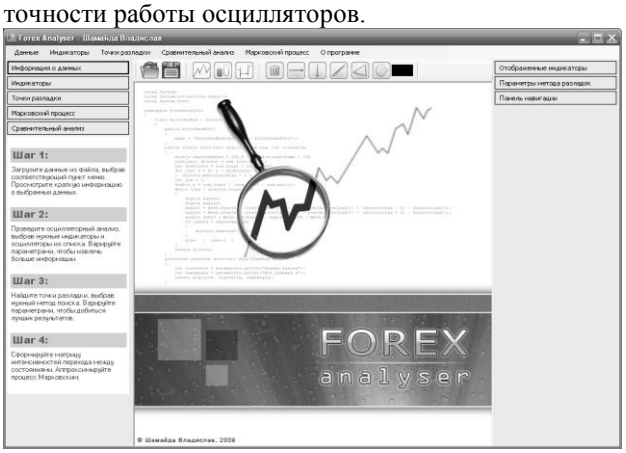


Рисунок 2. Главное окно программы «Forex Analyser»

Так, после проведения специально разработанного теста, было подтверждено запаздывающую реакцию скользящих средних WMA и EMA, и заблаговременные показания не следующих за трендом осцилляторов, например, таких как Awesome Oscillator, Accelerator Oscillator, Range of Change. Но благодаря тому, что эти осцилляторы выдают много ложных сигналов об изменении состояния рынка, то рекомендуется их совместное использование с индикаторами, следующими за трендом.

ВЫВОДЫ

По результатам сравнительного анализа для краткосрочных и среднесрочных прогнозов эффективнее использовать сглаживание B-сплайнами – они показывают наилучший результат в соотношении отклонение к сглаживанию. Для дальнесрочных прогнозов лучше подходит SMA (для котировок со слабо выраженным трендом и сильной зашумленностью EURCAD, EURCHF) и WMA и EMA (в случае котировок с сильно выраженным трендом и слабой зашумленностью, например, CHFJPY, USDCHF).

Среди не индикаторных методов поиска разладок критерии изменения среднего и изменения дисперсии выдают сравнительно худшее результаты, благодаря тому, что они являются методами последовательного определения разладок, что приводит к запаздыванию сигналов. Согласно приведенным критериям оценки метод «заключения в коридор» показал наиболее точные результаты и был избран для оценивания индикаторных методов поиска точек разладки.

Еще одной отличительной способностью данной работы является то, что в качестве технического анализа рынка используется его аппроксимация Марковским процессом.

ПЕРЕЧЕНЬ ИСТОЧНИКОВ

1. Кудренко Д. В. Анализ информационных технологий задачи оперативного анализа фьючерсных рынков: Обзор /О. Ф. Приставка, С. О. Смирнов, О. М. Хохольков/ - Днепропетровск: Наука и образование, 2003г.-91с.

2. Приставка О.П., Приставка, П.О., Смирнов С.О. Статистичний аналіз в АСОД. Відтворення розподілів.: Навч. Посіб. – Д.: РВВ ДДУ, 2000. – 112 с.

3. Князевский В. С., Житников И. В. Анализ временных рядов и прогнозирование. Ростов н/Д: Рост. гос. экон. акад., 1998. - 161с.

УДК 004

АНАЛИЗ ИНТЕГРИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПОСТРОЕНИЯ АЛГОРИТМОВ ЛИНГВИСТИЧЕСКОГО АНАЛИЗА

Ищук Павел Александрович,
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://pzks.nmu.org.ua, E-mail: boer@ua.fm

Рассмотрены интегрированные информационные системы построения алгоритмов лингвистического анализа, проанализированы их достоинства и недостатки, а также их направленность и применимость к языкам славянской группы.

Ключевые слова – лингвистический анализ интегрированные информационные системы, лингвистический алгоритм, интерфейс системы.

ВВЕДЕНИЕ

Для существующих и разрабатываемых программных средств, предназначенных для работы с естественным языком, функциональную основу составляют лингвистические алгоритмы, формализованные и реализованные в одном или нескольких языках программирования.

Именно от того, насколько полна и удачна конкретная реализация лингвистического алгоритма, лежащего в основе программного обеспечения, зависит конкурентоспособность и положение на рынке программного продукта.

ОСНОВНАЯ ЧАСТЬ

На сегодняшний день, лингвистический участок науки находится в состоянии интенсивного развития, активно осваивая новые, и углубляясь в уже существующие направления. Об этом свидетельствует внедрение новых специальностей и отраслей, интегрирование появляющихся технологий с лингвистическими дисциплинами, которые до сих пор были исключительно областью филологии.

Развитие вычислительных мощностей и ориентирование электронных вычислительных машин на персональное использование, обуславливает необходимость наличия прогрессивных алгоритмов анализа естественно языковых текстов [1].

В 90-х годах фирма Microsoft создала научную группу Natural Language Processing (NLP) group[2], целью которой является проектирование и создание компьютерных систем, ориентированных на обработку естественной человеческой речи. По описанию Microsoft системы должны анализировать, понимать и генерировать естественную человеческую речь. Однако, если с последними двумя пунктами они справляются довольно неплохо (убедиться в этом можно на примере распознавания голосовых команд и озвучивание на английском языке текста, реализованных в операционных системах Microsoft Windows), то в отношении первого можно сказать, что он является объектом постоянных исследований. Следует также отметить, что группа разрабатывает Natural Language Processing (NLP-системы) для английского, французского, немецкого, испанского, китайского, корейского и японского языков.

Как сообщают на сайте группы [3], минимальный размер оперативной памяти, необходимой для запуска Stanford CoreNLP составляет 2GB, система не обладает графическим интерфейсом, а работает через командную строку.

В конце 2001 года, фирма Text Analysis International выпустила интегрированную информационную систему Visual Text™ (рис 1).

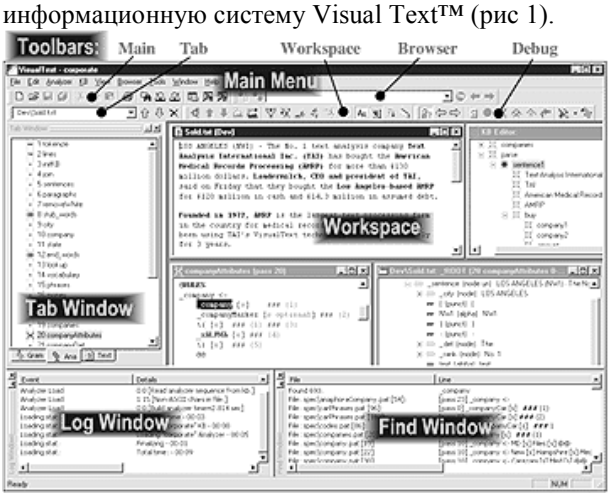


Рисунок 1. Интерфейс системы VisualText™

Внешне она имеет сходство с системой разработки Visual C++, но специализируется на NLP-обработке естественного языка. Исходя из слов авторов этой системы, язык программирования, применяемый в этой системе - NLP++, и являющийся её основой, позволяет запрограммировать «всё что угодно» (“anything thinkable can be programmed”), но на практике Visual Text ™ ограничен.

Открытая архитектура позволяет интегрировать программное обеспечение на NLP++ в программы на C++, но с другой стороны все алгоритмы и модели данных Visual Text™ являются закрытыми. Внутренняя составляющая Visual Text™ представляет собой черный ящик, что делает невозможным её полноценное использование и усовершенствование, а также, ориентацию на какой либо другой язык.

Недостатком этой системы является ее неинвариантность к объектам анализа. Например, невозможно с ее помощью создать алгоритм анализа ни украинского, ни русского, а также, другого языка славянской группы. Недостатком является, также, закрытость к расширению языка NLP++.

Обработкой естественного языка занимаются в

Университете Южной Калифорнии. Это Webclopedia проект, связанный с созданием информационных агентов, способных генерировать ответы пользователю на основе анализа разнородных коллекций ресурсов, доступных в сети. ONTOSAURUS – онтологический тезаурус, SUMMARIST – мультиязычная система реферирования текстовой информации, ReWrite – система двуязычного перевода, основанная на статистическом анализе пар текстовых корпусов.

Можно утверждать, что в России лингвотехнология уже сформировалась как отрасль информационных технологий, а такие фирмы как ABBYY, ПРОМПТ, ИНФОРМАТИК приобрели мировую популярность.

Среди украинских компаний, наивысших достижений в области лингвотехнологии получила компания ProLing с её продуктами: РУТА (проверка орфографии, грамматический контроль, расстановка переносов) и ПЛАЙ – программа российско-украинского и украинско-русского перевода. Эта система в процессе своей работы использует объектную модель Microsoft Office и встраивается в него в качестве надстройки.

ВЫВОДЫ

В результате проведённого исследования видно, что существующие интегрированные информационные системы, ориентированные на анализ естественного языка, либо строго коммерциализированны и обладают полностью закрытой архитектурой и предоставляют только интерфейс для их использования, либо ориентированы на более строго формализованные и менее инвариантные языки, как английский, французский, немецкий, испанский, китайский, корейский и японский языки. При этом, полностью открытой архитектурой, доступной к расширению и адаптации к другим языкам, ни одна из них не обладает.

Дальнейшие исследования необходимо направить на разработку системы, ориентированной на славянскую группу языков и обладающую развитым графическим интерфейсом, а также способностью к расширению функциональных возможностей.

ПЕРЕЧЕНЬ ИСТОЧНИКОВ

1. Бриллюэн Л. Наука и теория информации /Пер. с англ. – М., 1960. – 392с.; Волькенштейн М.В. Теория информации и эволюция// Кибернетика живого: Биология и информация. – М., 1984. – С. 45-53.

2. Microsoft NLP Group http://research.microsoft.com/en-us/groups/nlp/.

3. The Stanford Natural Language Processing Group http://nlp.stanford.edu/software/corenlp.shtml

Секція «Телекомунікації»

Голова секції: д.т.н., професор кафедри безпеки інформації та телекомунікацій Корнієнко В.І.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Рибальченко Ю.П.

УДК 004.73

МОДЕЛИРОВАНИЕ ПРОЦЕССА VOIP ТЕЛЕФОНИИ ПО GRE ТУННЕЛЮ

Кабак Д.С.[1], Магро В.И
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: kabakdmitry20@gmail.com[1]

Рассмотрена технология организации IP-телефонии по GRE туннелю между удаленными сетями. Проведена настройка и симуляция работы сети в среде GNS3. В качестве результата приведено содержимое пакетов установления логического канала для звонка.

Ключевые слова – моделирование; телефония; RGE туннель; удаленные сети.

ВСТУПЛЕНИЕ

На сегодняшний день существует всевозможное множество приложений и протоколов для организации VPN, но большая их часть является способами подключения хостов, а не сетей [1–3]. Подразумевается удаленная работа. Актуальной задачей является соединение не отдельных хостов, а целых локальных сетей. Одним из решений данной задачи является организация GRE-туннеля между сетями.

ОСНОВНИЯ ЧАСТЬ

Под IP-телефонией подразумевается голосовая связь, которая осуществляется по сетям передачи данных, в частности по IP-сетям (IP — Internet Protocol). На сегодняшний день IP-телефония все больше вытесняет традиционные телефонные сети за счет легкости развертывания, низкой стоимости звонка, простоты конфигурирования, высокого качества связи и сравнительной безопасности соединения. При осуществлении звонка голосовой сигнал преобразуется в сжатый пакет данных, далее происходит пересылка данных пакетов поверх сетей с коммутацией пакетов, в частности, IP сетей. При достижении пакетами получателя, они декодируются в оригинальные голосовые сигналы.

Добротность речевого трафика сильно зависит от качества передачи, и в сети, где не реализованы механизмы, гарантирующие соответственное качество, реализация IP-телефонии может быть не удовлетворяющей требованиям пользователей.

Основными показателями качества обслуживания являются пропускная способность сети и задержка передачи. Задержка при этом определяется как промежуток времени, прошедший с момента отправки пакета, до момента его приема.

Также существуют такие характеристики, как готовность сети и ее надежность (оцениваются по результатам контроля уровня обслуживания в течение длительного времени, либо по коэффициенту использования).

Для улучшения качества связи используются следующие механизмы:

1. Перемаршрутизация. При перегрузке одного из каналов связи позволяет осуществить доставку при помощи резервных маршрутов.
2. Резервирование ресурсов канала связи на время соединения.
3. Приоретизация трафика. Дает возможность помечать пакеты в соответствии с уровнем их важности и производить обслуживание на основе меток.

Например, необходимо создать защищенный канал между двумя удаленными офисами. Топология сети представлена на рис. 1

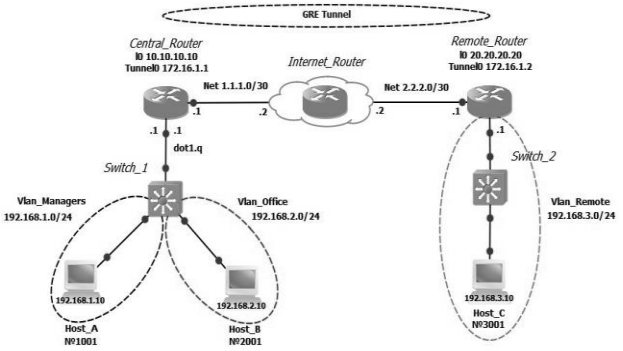


Рисунок 1. Топология сети

Есть центральный офис, в котором расположен роутер (Central Router) с поддержкой VoIP. Он подключен одним интерфейсом в локальную сеть, где имеется два vlan (Managers (192.168.1.0/24) и Office (192.168.2.0/24)). Центральный маршрутизатор является шлюзом по умолчанию для локальной сети. В этих сетях находятся рабочие станции для проверки (Host A и Host B). На них установлен Cisco IP Communicator и заданы телефонные номера (№1001 и №2001 соответственно). Вторым интерфейсом маршрутизатор подключен к интернету. Так же есть удаленный офис, в котором находится роутер Remote Router. Он тоже поддерживает VoIP и у него есть два интерфейса (один для внутренней

сети, один для интернета). Для удаленных пользователей есть выделенная сеть (Remote (192.168.3.0/24)), в которой установлена станция для проверки Host C с установленным Cisco IP Communicator и номером №3001, причем для этого пользователя организована двойная линия.

Для защиты телефонного трафика при прохождении через интернет будем использовать GRE туннель. Для его организации используются Tunnel интерфейсы на роутерах (Tunnel0 (172.16.1.1) – на роутере Central Router и Tunnel0 (172.16.1.2) – на роутере Remote Router). Телефонная сеть строится с помощью CME (Call Manager Express). Для задания IP-адреса, к которому будут обращаться наши Cisco – телефоны (Cisco IP Communicator) будем использовать loopback интерфейсы (l0 (10.10.10.10) – на роутере Central Router и l0 (20.20.20.20) – на роутере Remote Router). Вначале настраивается сетевой доступ коммутаторов. В режиме создания подсетей, конкретным подсетям присваиваются определенные порты коммутаторов. Коммутатор соединен с роутером при помощи trunk интерфейса с указанием имен подсетей с правами доступа к trunk.

Далее конфигурируются Central и Remote Router по следующему алгоритму (пример для Central Router):

1. Создать loopback интерфейс с IP адресом 10.10.10.10;
2. Создать sub-интерфейсы для ранее созданных подсетей и назначить им соответствующие IP-адреса;
3. Создать интерфейс, смотрящий в сторону интернета с адресом 1.1.1.1;
4. Создать интерфейс для GRE туннеля и назначить ему IP адрес 172.16.1.1;
5. Определить порт для начала GRE туннеля и IP адрес конца туннеля 2.2.2.1;
6. Задать маршрут к удаленной сети Remote через туннель.

Далее настраиваем протокол VoIP на каждом маршрутизаторе по следующему алгоритму.

1. Назначить максимальное количество телефонов, которое нам потребуется в нашей телефонной сети;
2. Назначить максимальное количество телефонных линий;
3. Назначить время, в течение которого CME будет ждать ответа от IP-телефона в случае обрыва связи, после которого он начнет попытку перерегистрации;
4. Задать IP-адрес и порт, на который будут обращаться IP-телефоны для регистрации;
5. Указываем роутеру создавать файл конфигурации в формате XML, который затем будет скачан IP-телефонами.
6. Создать логическую "телефонную" линию и задать номер, который будет ей соответствовать.
7. Создать первый IP телефон и задать ему mac адрес и другие настройки.
8. Создать шаблон переадресации звонка на соседний CME если номер начинается на "30".
9. Задать дополнительный маршрут к loopback-интерфейсу соседнего CME через интерфейс Tunnel 0. Таким образом, телефонный трафик инкапсулируется в GRE туннель.

Маршрутизатор Remote Router настраивается аналогично за исключением шаблона переадресации, т.к. он перенаправляет все звонки на соседний CME.

МОДЕЛИРОВАНИЕ

В процессе моделирования были созданы три виртуальных машины в среде Virtual Box с установленным на них ПО Cisco IP Communicator. Каждая из них была ассоциирована со своей подсетью: Office, Managers и Remote. Далее были произведены тестовые звонки между всеми участниками сети, чтобы проверить работоспособность настроенной конфигурации.

Для проверки работы GRE туннеля использовалась программа мониторинга пакетов Wireshark. На рис. 2 показан результат работы программы для пакета установления логического канала звонка.

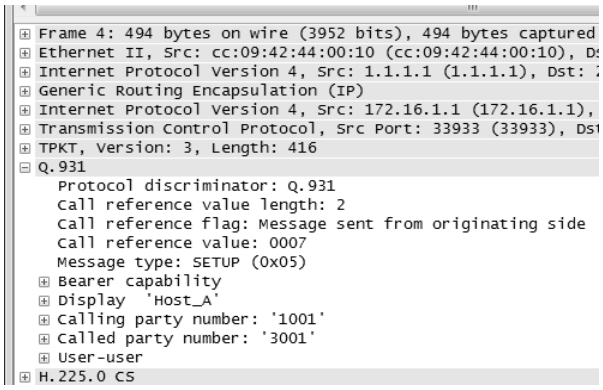


Рисунок 2. Содержимое пакета установки логического канала звонка

На рисунке 2 отчетливо видны уровни инкапсуляции первоначального пакета, протоколами GRE, IP, Ethernet и т.д. Эти заголовки в дальнейшем присутствуют в каждом пакете голосовой связи через VoIP из чего было заключено, что весь трафик идет через защищенный GRE туннель.

ВЫВОДЫ

В ходе моделирования была определена оптимальная конфигурация сети для организации голосовой связи VoIP с удаленной локальной сетью по защищенному GRE туннелю. Это позволяет использовать данную технологию в публичной сети, скрывая внутреннюю информацию пакетов. Однако данные инкапсулированные в GRE передаются в открытом виде, и это может стать угрозой безопасности приватных данных. Дальнейшее исследование должно быть направлено на организацию шифрования данных с целью защиты их от фальсификации

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы технологии протоколы. СПб.: Питер, 2010.— 916с.
2. Кларк К., Гамильтон К. Принципы коммутации в локальных сетях Cisco / К. Кларк, К. Гамильтон; под ред. Мысника А.В. - М.: Издательский дом «Вильямс». — 2003.- 976 с.
3. Гольдштейн Б.С. IP-телефония. М.: Радио и связь, 2001.— 336с.

УДК 621.39:006.91 (02)

ОЦІНКА ЯКОСТІ НАДАННЯ ПОСЛУГ В МЕРЕЖАХ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ

Бреславський В.О., аспірант,
Державний університет телекомунікацій, м. Київ, Україна, http://www.dut.edu.ua, E-mail: slaava@i.ua

Оцінка якості надання послуг в мережах стільникового зв’язку. Якість послуг зв'язку є тим фактором, який впливає на рівень конкурентоспроможності серед операторів зв'язку. Єдині показники якості надання послуг зв’язку будуть використовуватися як операторами зв’язку, так й представниками офіційної влади, фізичними та юридичними особами.

Ключові слова: методики, QoS, стандарти якості, обладнання, стільниковий зв’язок.

ВСТУП

На сучасному ринку послуг зв'язку, на якому попит на послуги зв'язку досяг насичення, основна увага операторів зв'язку спрямовано на розширення переліку послуг та підвищення їх якості.

Основним документом з якості є світовий стандарт якості ISO 9001: 2000, який визначає параметри за вимогами до продукції і містить основні та додаткові матеріали по пропонованим вимогам. Однак при цьому він не визначає параметри документації для даного продукту в системі менеджменту якості [1-2]. Міжнародний стандарт якості зв'язку містить основні вимоги, однак в ньому відсутній процес з підтримання стандарту якості послуг в мережах стільникового зв’язку.

Поліпшення менеджменту якості системи зв'язку є безперервним процесом з чіткими внутрішніми і зовнішніми зв'язками між споживачами і виробниками-постачальниками послуг зв'язку. Вимоги до переліку показників якості послуг зв'язку можуть встановлюватися в стандартах міжнародних організацій, таких як MCE, ETSI, національних стандартах, галузевих стандартах та інших документах.

Моніторинг якості послуг зв'язку здійснюється шляхом вимірювання на мережі зв'язку, які можуть спиратися на статистичні дані або контрольні вимірювання, так і на підставі опитувань користувачів послугами зв'язку та аналізу поданих ними претензій.

Результатами моніторингу якості послуг зв'язку є:

- повідомлення регулюючого органу на Web-сайті, в прес-релізах;
- публікації в засобах масової інформації;
- накладення адміністративного штрафу;
- судові розгляди.

Одним з найважливіших показників якості послуг є **Quality of Service** або **QoS**. Зазначене - є системою з визначення рівня якості обслуговування.

QoS регулює і керує всіма процесами в мережі - від послуг та бізнесу до елементів робочих мереж. Отже, клієнт отримує гарантовано замовлений рівень якості надаваних послуг зв'язку, незалежно від будь-якого трафіку. З цього випливає, що високопріоритетні послуги надаються за вищими тарифами і їх кількість нижче стандартних послуг і користувачів з вищим пріоритетом, ніж користувачів з стандартними вимогами. Прикладом користувачів з вищим пріоритетом можна назвати служби мультимедіа. QoS використовується з різними протоколами, існуючими на сьогоднішній день, що включає в себе кілька видів технологій, які дозволяють максимально ефективно і доцільно використовувати існуючі ресурси[3-4].

Проблема роботи QoS в системі LAN - відсутність підтримки останніми якості обслуговування, оскільки пріоритет користувача не може бути рівний пріоритету доступу.

В свою чергу QoS в VoIP ділиться на чотири класи. Класифікація включає в себе мережеві та термінальні параметри та характеристики.

1. Вищий клас припускає використання широкосмугових кодеків і мереж, які відповідають європейським вимогам QoS.

2. Високий клас припускає використання мереж з бездротовими системами мобільного зв'язку, кодеків EFR і MCE-T G.726. Впровадження систем допустимо для високого відсотка користувачів - більше 85%.

3. Середній клас припускає використання кодеків FR. На момент впровадження допускалося його використання для невеликої кількості абонентів - не більше 10%.

4. Доступний клас прийнятний для використання, проте не гарантує підтримку характеристик з'єднання. Рекомендації QoS до нього незастосовні, діалогова інтерактивність низька і мовний зв'язок на низькому рівні якості. Використовувати можна тільки у виняткових ситуаціях при загальному відсотку користувачів не більш 5%.

Варто відзначити, що сучасні технології що створенні, розроблені та впровадженні для QoS дозволяють застосовувати її як в мережах GSM, так і в телекомунікаційних послугах зв'язку в цілому - мобільної, аматорської, супутникової та Інтернет.

До основних показників QoS в мережах стільникового зв’язку відносять:

- Покриття поза будівлями і всередині будівель.
- Відсоток викликів, які закінчилися роз'єднанням встановленого з'єднання без ініціативи абонента.
- Відсоток неуспішних викликів.
- Час, витрачений на встановлення з'єднання.

Є також більш детальна класифікація показників якості послуг рухомих мереж. Крім цього, розроблені і впроваджені норми за показниками якості

надаваних послуг[4].

Для оцінки та визначення зазначених параметрів розроблені спеціальні методики і алгоритми, що відповідають вимогам до програм, які призначені для оцінки показників якості. Нормативи за результатами випробувань діляться на дві категорії - або високий, або нормальний. Оцінка технічних показників дозволяє визначити рівень якості послуг в рухомих мережах і відповідність показників заявленим даним.

Також, до основних методів оцінки якості послуг на мережі операторів телекомуникацій відносять:

- активний чи інтрузивний - POLQA і PESQ;
- пасивний або неінтрузівний - P.563;
- модельований - E-model.

З метою більш детального дослідження процесу вимірювання параметрів якості послуг, що надаються в стільнікових мережах звязку, слід навести приклади найбільш разповсюджених вимірювальних приладів.

Устаткування для вимірювань - стаціонарні і мобільні тестові апарати і комплекси.

Як в будь-якій сфері вимірювань тестове обладнання може бути як стаціонарним, так і мобільним. Перевагою стаціонарних комплексів є їх потужніть та більша кількість агентів (датчиків, індикаторів), які розташовані у різних сегментах мережі та дістанційно керуються стаціонарним комплексом моніторингу. Переносні, мобільін комплекси монітронгу мають можливість зідснювати вимірювання в тих місцях, де в цьому є критична необхідніть (під час аварій, у труднодоступних сегментах мережі).

ВИСНОВОК

Операторам телекомунікацій слід більше уваги приділяти параметрам якості послуг. Одним з найважливіших показників, на який слід звернути увагу – **QoS**. Крім того, необхідно проводити вимірювання параметрів якості телекомунікаційних мереж на постійному рівні. Під час проведенні вимірювань необхідно використовувати затверджені методики та відповідні параметри тестування. Так, для тестування голосових сервісів слід використовувати контрольні виклики наступних проміжків часу: 10 секунд - для тестування фази встановлення з'єднання; 120 секунд - для інших тестів. Під час збору даних випробувань за допомогою технічних комплексів збір даних доцільно проводити в безперервному режимі - випробувальний комплекс запускається, і сеанс випробувань закінчується або після закінчення тестового маршруту, або після закінчення строків проведення випробувань. Якщо контрольні виклики, що проводяться з тестових комплексів, фіксуються автоматично, спеціальної вимірювальної апаратурою на довготривалому носії, то всі результати і допоміжна інформація повинні зберігатися в зрозумілому вигляді, що дозволяє їх використовувати для обробки і аналізу. Результати вимірювань повинні бути по можливості відтворені, тому умови, при яких результати вимірювань були одержані, також повинні бути зафіксовані. До таких умов відносяться дата та час випробувань, маршрут, номери ISDN автовідповідачів і IP-адреси серверів[5-7].

Доцільно розробити універсальну систему моніторингу якості послуг, яка надасть можливість гнучко та оперативно відстежувати проблеми з якістю надання послуг зв’язку. Для цього доцільно використовувати платформу на основі комплексних систем моніторингу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ETSI, EG 202 057-3 "Обробка мови, передачі та аспекти якості: Параметри QoS, визначення та вимірювання, що відноситься до користувача; Частина 3: Параметри QoS для мереж стільникового наземного зв'язку", (Speech Processing, Transmission and Quality Aspects (STQ); User related QoS parameter definitions and measurements; Part 3: QoS parameters specific to Public Land Mobile Networks (PLMN)), 2005.
2. MCE-P, "Вимоги до продуктивності і якості сервісу мереж доступу IMT-2000" (Performance and quality of service requirements for International Mobile Telecommunications-2000 (IMT-2000) access networks), 2003.
3. TRAI, "Стандарти якості послуг основних телефонних сервісів і правила для послуг мобільних телефонних мереж" (The standards of quality of service of basic telephone service (wireline) and cellular mobile telephone service regulations), 2009.
4. IDA, "Стандарти якості телефонних мобільних мереж 2G" (2G Public Cellular Mobile Telephone Service QoS Standards).
5. "Обробка мовлення, передачі та аспекти якості: Параметри QoS, визначення і вимірювання, що відноситься до користувача; Частина 2: Голосова телефонія, факс, модем, передача даних і SMS", (Speech Processing, Transmission and Quality аспекти (STQ); User related QoS parameter definitions and measurements; Part 2: Голосова телефонія, Group 3 fax,modem послуг передачі даних і SMS), 2005.
6. OFCOM, "Консультації по параметрам якості" (Consultation on quality parameters), 2004.
7. MCE-T, Рекомендація E.802, "Принципи і методики визначення та застосування параметрів Q S", 2007.

УДК 621.391

ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Рибіна Яна Андріївна[1]
Науковий керівник: проф. Корнієнко Валерій Іванович
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: yrybina9@gmail.com[1]

Розглянуто технологію передачі інформації за протоколом PWE3, що забезпечує вибір оптимального способу маршрутизації у комутаційному центрі для покращення якості обслуговування інформаційних потоків в мультисервісних мережах зв'язку.

Ключові слова - протокол PWE3, трафік, інформаційні потоки, комутаційний центр.

ВСТУП

На сьогоднішній день актуальним є забезпечення заявленого рівня якості обслуговування абонентів в мережах мобільного зв'язку.

Проблема ускладнюється тим, що спектр послуг, що надаються, розширюється з кожним днем, а це передбачає передачу великих об'ємів інформації різного типу з різними вимогами до якості передачі.

Зростання об'ємів трафіку потребує ефективної передачі інформації. Перспективні моделі та методи оцінки якості обслуговування інформаційних потоків повинні враховувати різнорідну природу трафіку, що передаються, при цьому повинні бути максимально адаптовані до протоколу, за яким здійснюється передача.

МЕТОДИКА ДОСЛІДЖЕННЯ

Однією з перспективних технологій для передачі інформації вважається протокол PWE3 (Pseudo Wire Emulation Edge-to-Edge). Він здійснює з'єднання між комутаційними центрами, до яких підключені базові станції, та контролером базових станцій через мережу з комутацією пакетів [1].

Завданням PWE3 є забезпечення мінімальної необхідної функціональності для передачі з необхідною мірою достовірності для даного типу сервісу. За реалізацію всіх функцій комутації відповідає механізм пересилки (FWRD - Forwarder).

Аналіз роботи мереж за протоколом PWE3 показав, що розподіл інформаційних потоків від базових станцій є недостатньо ефективним. Передача здійснюється таким чином, що для кожної базової станції прокладається окремий тунель – логічний канал, по якому здійснюється передача всіх інформаційних потоків від однієї базової станції (рис. 1). Така схема неефективна через те, що навантаження на базові станції залежно від часу може змінюватися.

Це обумовило виникнення задачі оцінки якості обслуговування інформаційних, що полягає у передачі сумарного інформаційного потоку від всіх базових станцій по всіх тунелях, що з'єднують два комутаційні центри PE1 та PE2.

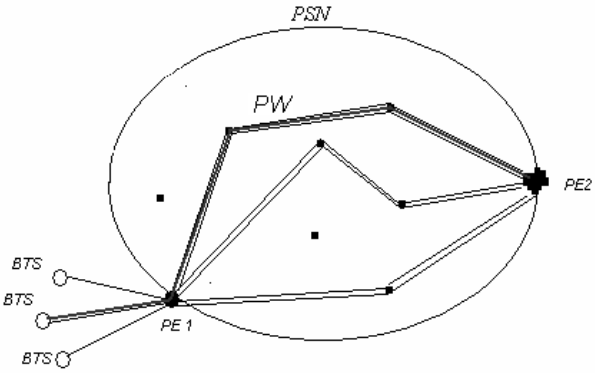


Рисунок 1. Організація PWE3

На рис. 2 показана схема роботи комутаційного центру, де видно, що всі вхідні потоки, які поступають на вхід до комутаційного центру спершу комутуються, тобто розподіляються по каналах зв'язку, а потім класифікуються та утворюють черги відповідно до типу трафіку.

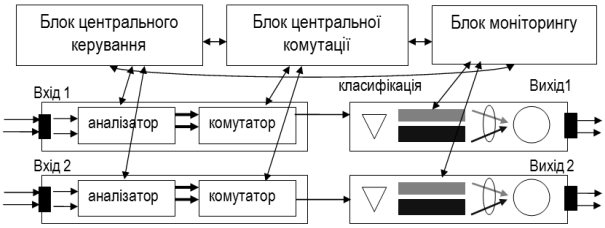


Рисунок 2. Схема обробки заявок в комутаційному центрі

У зв'язку з тим, що маршрутизація інформаційних трафіків від PE1 до PE2 в комутаційному центрі мережі PWE3 здійснюється за принципом «точка-точка», то система має змогу повністю контролювати характеристики трафіку. З метою зменшення втрат пакетів в чергах вихідних каналів схема роботи комутаційного центру PE удосконалюється за рахунок перенесення блоку класифікації до «аналізатора», який передує «комутатору», як показано на рис. 3.

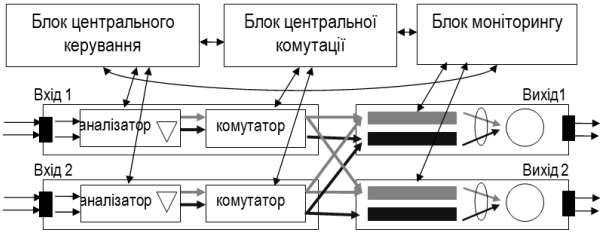
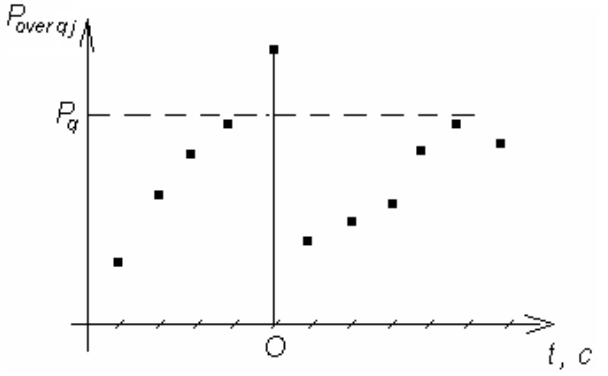
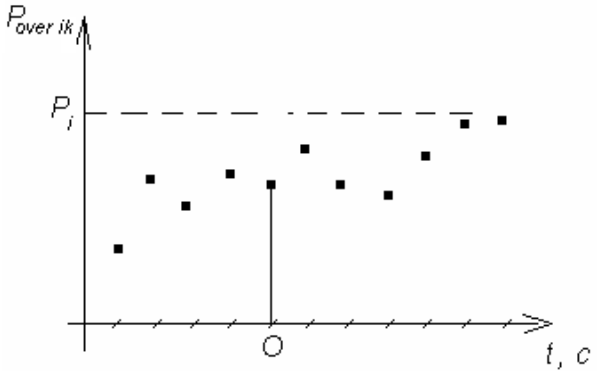


Рисунок 3. Вдосконалена схема роботи комутаційного центру

Класифікація трафіку до процесу комутації дозволить керувати наповненням черг заданих класів трафіків у вихідних каналах в залежності від поточного значення показника втрат пакетів у чергах за інформацією від блоку моніторингу. У разі переповнення черг в системі розв'язується задача вузлової маршрутизації для вибору каналу PW (Pseudo Wire), в якому буде організовано віртуальне з'єднання на час передачі інформаційної заявки.



а) трафік *q*



б) трафік *i*

Рисунок 4. Характер залежності втрат пакетів від часу.

Результат розв'язку задачі вузлової маршрутизації схематично зображений на рис. 4, де *O* – момент виникнення пікового навантаження, P_q, P_i – максимально допустимі втрати пакетів, *k* – номер вихідного каналу. На рис. 4 (а) показаний характер залежності втрат пакетів *q* (трафік, для якого зафіксовано перевантаження) в каналі *j* від часу. На рис. 4 (б) - характер залежності втрат пакетів трафіків *i* від часу.

Після сигналізації про перевантаження здійснюється перерозподіл інформаційних потоків між вихідними каналами зв'язку відповідно до задачі вузлової маршрутизації. Це спричиняє зменшення втрат пакетів трафіку, для якого було виявлено перевантаження, за рахунок незначного збільшення втрат пакетів решти трафіків в вихідних каналах зв'язку [2,3].

ВИСНОВКИ

Запропонований засіб підвищення якості обслуговування інформаційних потоків в мультисервісних мережах зв'язку шляхом передачі заявок від базової станції не по одному, а по всім вихідним напрямкам, що підвищує ефективність передачі комбінованих інформаційних потоків в комутаційних центрах на границі мережі мобільного оператора та орендованої мережі з комутацією пакетів. Таким чином, одночасно забезпечується підтримка необхідних рівнів якості передачі для різного типу трафіку.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Энциклопедия сетевых протоколов. Электрон. ресурс) / Способ доступа URL: http://www.protocols.ruWP/?p=1378;

2. Глоба Л.С. Модель управления информационными потоками в сетях с реализацией эмуляции постоянного соединения (PWE3) / Глоба Л.С. Скулиш М.А. // Материалы 18-й Международной Крымской конференции "СВЧ-техника и телекоммуникационные технологии" (КрыМиКо'2009). – г. Севастополь. – 2009. – С. 348-351.

3. Скулиш М.А. Метод оцінки якості обслуговування інформаційних потоків в мультисервісних мережах зв'язку / Автореферат дисертації на здобуття наукового ступеня Кандидата технічних наук. – м. Київ. – 2010.

УДК 681.3+681.7.068

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

Сикора Д.Н.[1], Рыбальченко Ю.П.
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: sikoradima84@gmail.com[1]

Рассмотрены особенности и реали волоконно-оптических линий связи. Приведен метод реконструкции волоконно-оптических линий связи, который позволяет существенно увеличить её пропускную способность.

Ключевые слова – Волоконно-оптическая линия связи, пропускная способность, маршрутизатор, коммутатор , пигтейл.

ВВЕДЕНИЕ

В связи с возрастающими потребностями клиентов, волоконно-оптические линии связи совершенствуются довольно быстро. При этом находящиеся в эксплуатаци оптоволоконные линии связи не всегда соответствуют современным требованиям, в связи с ограниченными их возможностями. Развитие оптоволоконной связи

требует решения задач эффективного усовершенствования существующих линий связи с многократным увеличением их пропускной способности. Данные задачи могут быть решены путем применения методов усовершенствования волоконно-оптических линий связи, находящихся в эксплуатации.

ОСНОВНАЯ ЧАСТЬ

Волоконно-оптическая связь - вид связи, который для переноса информационного сигнала использует электромагнитное излучение оптического диапазона. Распространение сигнала происходит по волоконно-оптическим кабелям. Несущая частота высокая, а мультиплексирование имеет широкие возможности, поэтому пропускная способность волоконно-оптических систем гораздо выше, чем пропускная способность всех других систем связи. Максимальные ее значения достигают терабит в секунду. Оптическое волокно характеризуется малым затуханием света, что способствует применению волоконно-оптических систем связи на больших расстояниях. Такой вид связи не чувствителен к внешним электромагнитным помехам, а также защищен от несанкционированного использования, поэтому перехватить сигнал, передаваемый по оптическому кабелю, невозможно.

Современное оптоволокно, которое используется в оптоволоконных системах, представляет собой прозрачные стеклянные волокна, которые проводят свет от одного конца к другому с минимальными потерями, благодаря эффекту полного внутреннего отражения. Что касается конструкции, то оптическое волокно состоит из ядра, оптической оболочки и защитной оболочки. Ядро и оптическая оболочка чаще выполнены из стекла, иногда - пластика, защитная оболочка, как правило, из пластика. Функция ядра оптоволокна состоит в пропускании светового сигнала, а оптической оболочки - в обеспечении полного внутреннего отражения света в ядре и его прохождении по всей длине. Защитная оболочка необходима для защиты ядра и оптической оболочки от внешних воздействий. Толщину оптического волокна можно сравнить с толщиной человеческого волоса (125 мкм - оптоволокно, 85 мкм - волосы).

Рассмотрим реальную волоконно-оптическую линию связи, которая используется ЧАО «Орель-Лидер». Контроль за роботой и управление всей телекоммуникационной сети происходит с помощью маршрутизатора «Cisco 2800» и двух коммутаторов: «Nortel 3510-24» и «Nortel 2550T». Непосредственно работа оптоволоконной линии связи осуществляется с помошью шести медиаконвертеров «D-Link DMC-1910R» - три из них находятся в главном здании, откуда ведется контроль и управление, и по одному в каждом из сооружений, к которым подведена волоконно-оптическая связь. По восьмижильным оптическим кабелям сигнал передается от одного медиаконвертера к другому. После приема оптического сигнала медиаконвертер проеобразовывает среду сигнала и на коммутаторы поступает электрический сигнал, который разделяется и направляется на персональные комптьютеры. [3]

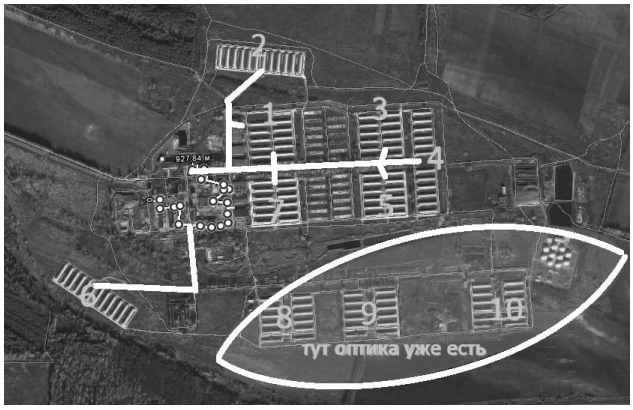


Рис. 1 – Схема существующей телекоммуникационной сети

Сложность и недостаток существующей сети состоит в том, что количество зданий, которые нужно подключить к оптоволоконной связи, двадцать одно, а реально подключены только три из них. Остальные соединены с помощью обычных DSL-модемов. При такой связи для соеденения сооружений используется тип кабеля - «витая пара». Широко известно, что кабели такого вида имеют существенные недостатки[2]:

- сильное воздействие внешних электромагнитных наводок;
- возможность утечки информации;
- сильное затухание сигналов;
- проводники витой пары подвержены поверхностному эффекту;
- возможность простого несанкционированного подключения к сети.

Эти недостатки приводят к дополнительному ослаблению сигнала. В данный момент между сооружениями скорость передачи информации в среднем достигает 800 кбит/с.

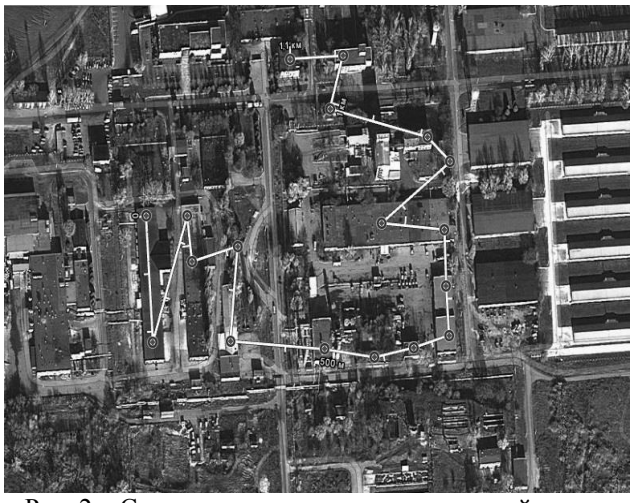


Рис. 2 – Схема проведения опто-волоконной линии связи.

Организация телекоммуникационной сети в таком виде не соответствуют растущим потребностям клиента, поэтому возникает необходимость усовершенствования всей сети и волоконно-

оптический линии связи, в частности.

Проанализировав особенности построения существующей телекоммуникационной сети, предлагается вариант её усовершенствования.

Во-первых, заменить маршрутизатор для контроля за работой и управлением сети: вместо «Cisco 2800» выбран более современный интеллектуальный Ethernet-коммутатор «Cisco Catalyst 2960». [3]

Во-вторых, непосредственно работа оптоволоконной линии связи осуществляется с помошью сорока двух медиаконвертеров «4A FORA FMC-101»: половина из них находятся в главном здании, остальные - по одному в каждом из сооружений, которые подключаются к волоконно-оптической линии связи. Ранее используемый восьмижильный оптический кабель заменён на двадцатичетырёхжильный. Он начинает проводиться из главного здания. Каждая жила заводится в отдельное здание и с помощью пигтейлов подсоединяется к медиаконвертеру, от которого по кабелю типа «витая пара» электрический сигнал поступает на коммутатор. Коммутаторы так же заменены: выбраны «D-Link DES-1008A». После разделения электрический сигнал поступает на персональные компьютеры.

После усовершенствования таким образом существующей волоконно-оптической линии связи пропускная способность её увеличилась многократно: вместо прежней скорости передачи информации внутри линии, величина которой была в среднем до 800 кбит/с, получена новая средняя скорость передачи информации – до 100 Мбит/с.

ЗАКЛЮЧЕНИЕ

Установлено, что увеличение пропускной способности волоконно-оптической линии связи зависит от типа кабеля для прохождения оптического сигнала и используемого для его формирования оборудования. Показано, что при усовершенствовании существующей оптоволоконной линии связи пропускная способность существенно увеличивается.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco IOS IP SLAs Configuration Guide/2008. — 156 с.
2. Основные особенности сетевых кабелей http://netcab.narod.ru
3. Хилл Брайан. Полный справочник по Cisco / Брайан Хилл // Издательский дом «Вильямс». —2004

УДК 004.772

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ ПАКЕТНОГО ТРАФИКА

Осадчая Валентина Павловна[1],

Научный руководитель: к.ф.-м.н. Гусев Александр Юрьевич[2]

Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,

http://bit.nmu.org.ua, E-mail: valia.osadchaya@yandex.ua[1], gusev1950@mail.ua[2]

В работе рассматривается самоподобный трафик и его влияние на качество обслуживания. Приведен результат исследования реального самоподобного трафика.

Ключевые слова – самоподобный трафик; качество обслуживания; задержка; параметр Хёрста.

ВВЕДЕНИЕ

Пакеты при высокой скорости их движения по сети поступают на узел не по отдельности, а целой пачкой. Трафик в таких сетях имеет явно выраженный всплесковый характер, что повышает вероятность перегрузок в узлах сети, которые ведут к переполнению буферов и вызывают потери и /или задержки. Пульсации приводят к перепадам скорости информационных потоков, при которых отношение максимального значения к минимальной скорости составляет десятки раз. Однако, как оказалось, в мультисервисных сетях число событий на заданном временном интервале зависит от прежних, весьма отдаленных событий. Это означает, что при больших масштабах мультисервисной сети трафик обладает свойством самоподобия, т.е. выглядит качественно одинаково при любых достаточно больших масштабах временной оси.

Требуемое качество обслуживания потребителей услуг при реальном самоподобном трафике обеспечивается путем перераспределения пропускной способности устройств.

Под качеством обслуживания понимают интегральный полезный эффект от обслуживания, который определяется степенью удовлетворения пользователя как от полученной услуги, так и от самой системы обслуживания. Критерий качества обслуживания представляется в виде интегрального показателя совершенства обслуживания, учитывающего не только качество услуги, но и способность сети обрабатывать реальную нагрузку.

На качество обслуживания в IP-сетях влияют следующие основные факторы:

1. Задержка – время, которое требуется пакету для его передачи из одного пункта в другой. Эта величина зависит от доступной полосы пропускания, загрузки ресурсов сетевых устройств, расстояния между узлами. Время задержки речевого трафика состоит из: задержки на кодирование и декодирование в шлюзах, и задержки, вносимые сетью (в маршрутизаторах, линиях связи). Уменьшить задержки можно за счет проектирования инфраструктуры сети с минимальными задержками и

за счет уменьшения времени обработки информационного трафика в шлюзе и/или на транспортном узле;

2. Джиттер – вариация задержки находится в прямой зависимости от загруженности каналов;

3. Потеря пакетов происходит при перегрузке сетей или устройств;

4. Контроль над использованием полосы пропускания.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Был проведен анализ статистических характеристик реального трафика пакетов отдельных протоколов и всего трафика в целом. Реальный поток сформирован множеством источников: DHCP, IGMP, MPEG-1 Audio, MPEG video-stream, ARP, STP, UDP и другие. Измеренные данные свидетельствуют о том, что для трафика характерна сильная неравномерность интенсивности поступления заявок и пакетов. Заявки и пакеты рассредоточены в различных интервалах времени и могут группироваться в «пачки» в одних интервалах, а также полностью отсутствовать в других интервалах времени (рисунок 1 и рисунок 2).

В пачечном трафике при небольшом среднем значении интенсивности поступления пакетов (интенсивность трафика) присутствует достаточное количество относительно больших выбросов.

Для потока MPEG-1 Audio средняя интенсивность поступления составляет 19,8 пакетов в минуту за интервал 270 минут, а отдельные выбросы составляют 92 пакетов в минуту. В таблице 1 представлены вычисленные количественные характеристики реального трафика.

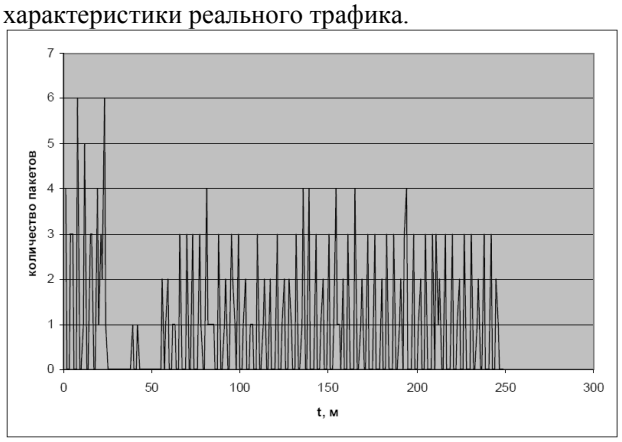


Рисунок 1. Интенсивность поступления пакетов IGMP

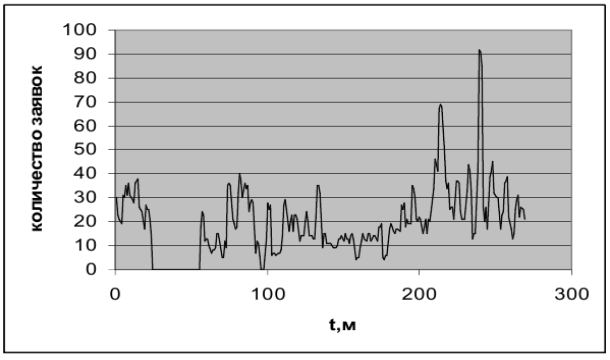


Рисунок 2. Интенсивность поступления пакетов MPEG-1 Audio

Таблица 1. Статистические характеристики реального трафика

Наименование	**IGMP**	**MPEG-1 Audio**	**DHCP**	**ARP**	**Общий**
Математическое ожидание	0,887	19,33	1,012	1,89	0,0021
Дисперсия	196,3	502,12	270,9	865,2	0,0002
Среднеквадратическое отклонение	14,04	22,41	16,46	29,41	0,015
Коэффициент вариации	15,82	1,159	16,46	15,51	7,12
Интенсивность	0,015	1,331	0,017	0,03	17,195

Результаты исследований показывают, что интенсивность трафика представляет собой случайный процесс, который имеет флуктуации (пачечность, пикфактор) во времени. При этом даже протокол TCP, гарантирующий надежную передачу последовательности пакетов, может не обеспечить качество обслуживания в «моменты» пиковой нагрузки сети.

Разброс интервала времени между требованиями определяется по формуле:

$$S = \frac{\sigma^2}{\Lambda}, \qquad (1)$$

где S – коэффициент скученности нагрузки или пик-фактор трафика; Λ – интенсивность; σ^2 – среднеквадратическое отклонение.

Анализ коэффициента скученности однородных потоков показал, что σ^2 превышает Λ от десятков до сотен раз. Из-за этого в пачечном трафике при сравнительно небольшом среднем значении интенсивности поступления пакетов присутствует определенное количество относительно больших выбросов.

Исследование объединенного трафика реального времени на самоподобие методом нормированного размаха показал, что параметр Хёрста H равен 0,9; для однородных потоков ARP и DHCP показатель H равен соответственно 0,85 и 0,86.

В [1] показано, что для описания трафика в мультисервисных IP-сетях наиболее широко используют распределения с тяжелым хвостом, в частности, распределение Парето, в которых параметр потока α характеризующий «тяжесть» хвоста распределения и определяет пачечную структуру процесса.

Для измеренного трафиков запросов ARP и DHCP определены «тяжесть хвоста» α равный соответственно 1,5453 и 1,434.

На рисунке 3 показано, что с увеличением параметра H растет задержка обработки трафика маршрутизатором. Время задержки, вносимое сетью можно уменьшить за счет приоритетного обслуживания соответствующих требований или рациональным выбором типа маршрутизатора[2].

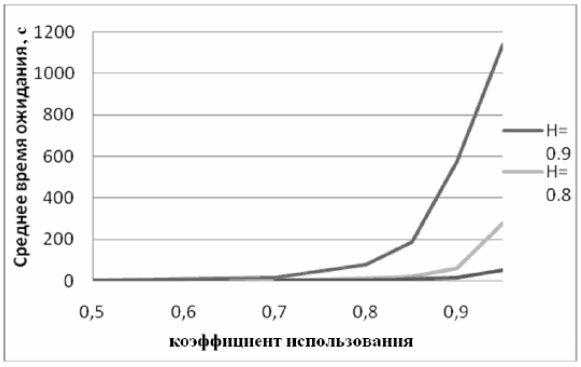


Рисунок 3. Зависимость времени задержки от загрузки пропускной способности маршрутизатора самоподобным потоком

ВЫВОДЫ

С увеличением параметра Хёрста мультисервисного потока канал связи не способен пропустить самоподобный трафик задержки передаваемой информации, а также растет время задержки отработки трафика маршрутизатором.

Критерий качества обслуживания пользователей услуг определяется способностью канала и сети связи без задержки обрабатывать самоподобный трафик.

Время задержки, вносимые каналом связи и сетью связи при самоподобном трафике можно уменьшить путем повышения широкополосности канала связи и за счет установления приоритетов обслуживания трафика, а также рациональным выбором типа устройств обработки трафика (маршрутизатора).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Шелухин О.И., Тенякшев А.М., Осин А.В. Фрактальные процессы в телекоммуникациях – М.: Радиотехника, 2003. – 480 с.

2. Осин А. В. Влияние самоподобности речевого трафика на качество обслуживания в телекоммуникационных сетях – М.: Дисертация, 2005. – 164 с.

УДК 004.415.53

СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ И ЭМУЛЯЦИЯ CISCO В ГРАФИЧЕСКОМ РЕДАКТОРЕ GNS3

Еник Н.Б[1]., Магро В.И.[2]
Научный руководитель: канд. физ-мат. наук, доц. Магро В.И
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: samsungx666@mail.ru[1] magrov@i.ua[2]

В работе представлены возможности программы GNS3 в качестве доступной системы эмуляции.

Ключевые слова – эмуляция, GNS3, компьютерные сети, маршрутизатор, роутер.

ВВЕДЕНИЕ

В настоящее время индустрия телекоммуникационного оборудования развивается довольно стремительно, массы учреждений в избытке квалификационных специалистов. Умение быстро осваивать новые оборудования служит одним из требований рынка. Возможность, которую дает нам GNS3 это перенести учебный процесс в виртуальную среду, и эмулировать там реальные компьютерные сети и устройства. GNS3 – это программное обеспечение, имеющее понятный графический интерфейс, которое эмитирует сложные сети, и дает возможность эмулировать разные устройства такие как коммутатор, маршрутизатор, роутер и т.д. GNS3 может работать на разных операционных системах такие как Windows, MacOS и Linux.

ОСНОВНАЯ ЧАСТЬ

Рассмотрим локальную и удаленную сеть. У каждого маршрутизатора R1 и R2 есть своя локальная сеть, и эти маршрутизаторы соединены между собой информационной сетью. В таких сетях можно легко исследовать потерю пакетов. Для этого будем использовать запрос ICMP-Echo или Ping. Этот запрос позволяет проверять соединения в сетях на основе TCP/IP протокола. Для исследования процессов сети мы будем отправлять запросы на указанный адрес сити с помощью команды Ping и фиксировать полученные ответы от него. Ping – является утилитой для проверки соединения в сетях на основе стек протоколов (TCP/IP). Эта утилита отправляет запрос (ICMP Echo-Request) протокола межсетевых управляющих сообщений (ICMP) указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). С помощью ICMP Echo можно измерить время отклика маршрутизатора Cisco, имеющий свой IP - адрес, и любого устройства, который тоже имеет IP - адрес.

Создание сети состояло из 4 пунктов:

- Настройка роутера R1 в сторону хоста 1 (интерфейс Fa 0/0).

```
R1
R1en
R1#conf t
R1(config)#int fa 0/0
R1(config-if)#description Link_to_host
R1(config-if)#ip address 172.16.10.3 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#
```

- Настройка роутера R1 в сторону роутера R2 (интерфейс Ser 1/0)

```
R1(config)#int serial 0/0
R1(config-if)#description Link_to_R2
R1(config-if)#clock rate 56000
R1(config-if)#ip address 172.16.20.1 255.255.255.0
R1(config-if)#no sh
```

R1(config-if)#exit
R1(config)#exit
R1#wr

- Настройка роутера R2 в сторону хоста 2.

R2>en
R2#conf t
R2(config)#int fa 0/0
R2(config-if)#description Link_to_host
R2(config-if)#ip address 172.16.10.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit

- Настройка роутера R2 в сторону роутера R1.

R2(config)#
R2(config)#int serial 0/0
R2(config-if)#clock rate 56000
R2(config-if)#ip address 172.16.20.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#description Link_to_R1
R2(config-if)#exit
R2(config)#int serial 0/1
R2(config-if)#clock rate 56000
R2(config-if)#ip address 172.16.20.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#exit
R2#wr

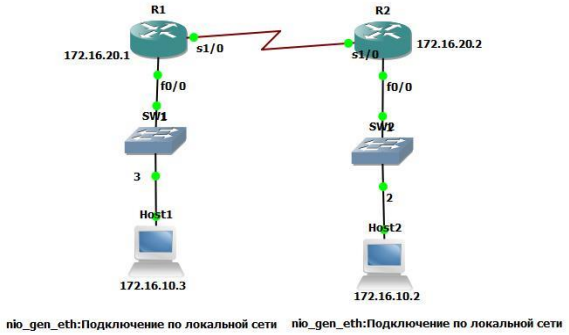


Рис. 1 – Принципиальная схема

При запуске роутера резко возрастает нагрузка на процессор для этого при помощи утилиты Idle-PC нужно снять нагрузку с ЦП, так как он поглощает 100% системной памяти процессора. Idle-PC это утилита которая погружает маршрутизатор в спящий режим до тех по пор пока мы с ним не начнем работу.

Мы протестировали сетевую доступность между роутерами, и хостами. На рисунке 2 изображено пингование сети, отправка пинга на хост 1, отправка пинга на роутер R2, отправка пинга на хост 2. Так же само сделали и со вторым роутером (Рис. 2). Увеличить скорость компьютерной сети можно разными способами. Можно коммутатор заменить на коммутатор.

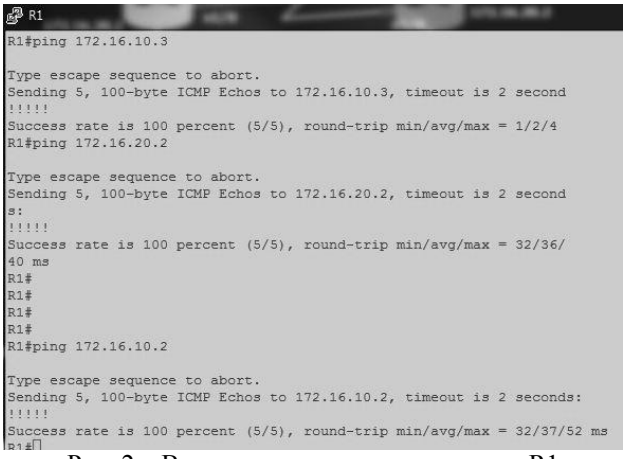


Рис. 2 – Выполнение команд на роутере R1

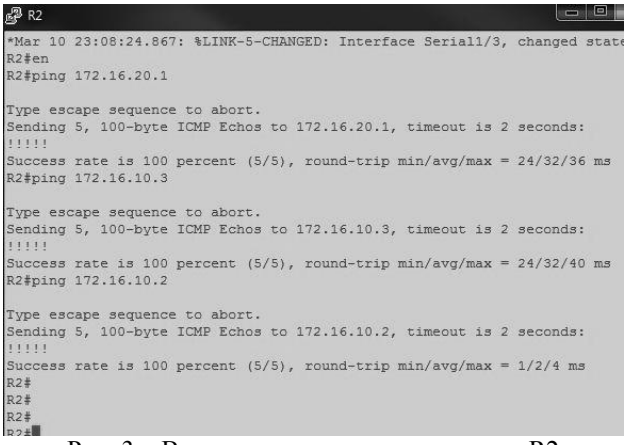


Рис. 3 – Выполнение команд на роутере R2

Коммутатор обладает специальным алгоритмом обработки сетевого трафика, который позволяет исключить отправку файлов по неверному адресу. Так же нужно проверить пропускную способность каналов. Это связано с тем, что скорость подключения к сети конечных станций намного превышает скорость канала связи между подсетями, в результате чего канал связи становится узким местом данной сети.

ЗАКЛЮЧЕНИЕ

Как видим GNS3 отличная платформа для экспериментов, тестов и изучение сетевых технологий. Процесс развития и эволюционирования различных платформ для эмуляции не стоит на месте, и вполне возможно, что в будущем мы получим единую среду, где будет возможно запускать и строить стенды, содержащие оборудование самых разнообразных компаний.

СПИСОК ЛИТЕРАТУРЫ

1. Официальное руководство Cisco / Уэнделл Одом / 2005
2. Хилл Брайан. Полный справочник по Cisco / Брайан Хилл //—2004
3. Олифер В.Г. Олифер Н.А. / Компьютерные сети. Принципы технологии протоколы / 2010

УДК 004.056.57

ОБРАБОТКА ИЗОБРАЖЕНИЙ РУДЫ В СИСТЕМЕ ВИДЕОМОНИТОРИНГА ГОРНОРУДНОГО ПРОИЗВОДСТВА

Левицкая Юлия Олеговна
Государственный ВУЗ «Национальный горный университет», г. Днепропетровск, Украина,
http://bit.nmu.org.ua, E-mail: julialev29@gmail.com

В работе предложено использование усовершенствованного метода обработки изображений – морфологического. Он выполняется путем наложения на изображение структурообразующего элемента, без вычислений и сравнений значения яркости сначала с пороговой, потом с яркостью соседних элементов. Он является эффективным и более быстрым, чем логический алгоритм из-за меньшего количества вычислений.

Ключевые слова – гранулометрический состав, бинарное изображение, морфологическая фильтрация.

ВВЕДЕНИЕ

Процесс предварительной переработки руды состоит из следующих этапов: взрывные работы, транспортирование, дробление и измельчение. На каждом из этих этапов одной из важнейших задач является повышение эффективности операций, чего можно достичь за счет оперативного контроля основного технологического показателя руды – гранулометрического состава.

Контроль осуществляется телекоммуникационной системой мониторинга с определением гранулометрического состава по оптическому изображению поверхности руды [1].

Использование информации о текущем гранулометрическом составе руды на входе/выходе технологической операции позволяет оперативно изменять режимы работы технологического оборудования с целью обеспечения требуемых показателей производства.

Сама обработка изображений производится на приемнике и включает в себя подавление шума, повышение контраста, сегментацию, бинаризацию с морфологической фильтрацией изображения и вычисление гранулометрического состава руды.

МЕТОДИКА ИССЛЕДОВАНИЯ И РЕЗУЛЬТАТЫ

Алгоритм обработки реализован путем его моделирования в среде Matlab [2,3] на примере обработки кадров изображения крупнодробленой руды на конвейере, питающем мельницы самоизмельчения.

Алгоритм включает следующие процедуры:

1. Формирование исходного изображения (рисунок 1) :

```
a=imread ('ruda.jpg');
figure; imshow (a);
f=rgb2gray (a);
figure, imshow (f);
```

2. Логарифмическое преобразование яркости :

```
I=mat2gray (f, [0 83]);
gs = im2uint8 (I);
```

3. Применение фильтра Винера.

3.1. Моделируем пространственный фильтр:

```
PSF = fspecial ('motion', 7, 45);
```

Задаем параметры фильтра:

```
Sn = abs (fft2(gs)).^2;
nA = sum (Sn(:)) /prod (size (gs));
Sf = abs (fft2 (gs)).^2;
fA = sum (Sn (:))/prod (size (gs));
R = nA/fA;
```

3.2. Выполняем свертку изображения с заданным фильтром:

```
fr2 = deconvwnr (gs, PSF, R);
```

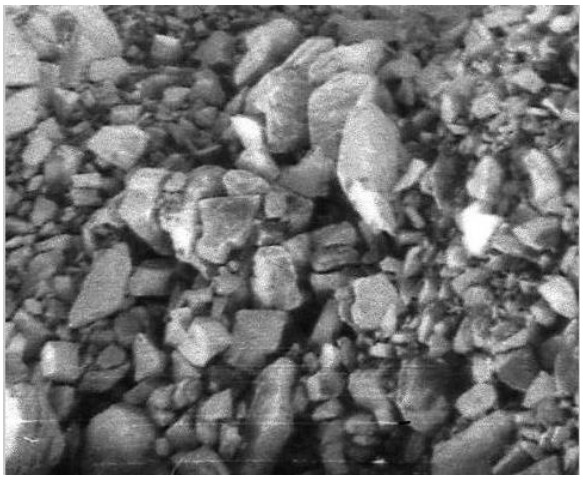


Рисунок 1. Исходное изображение руды

3.3. Фильтрация с использованием автокорреляционных функций:

```
NCORR = fftshift (real (ifft2 (Sn)));
ICORR = fftshift (real (ifft2 (Sf)));
fr3 = deconvwnr(gs, PSF, NCORR, ICORR);
z=mat2gray (fr3, [0 83])
gs3 = im2uint8 (z);
```

4. Подчеркивание границ – преобразование яркости и пространственная фильтрация:

```
w = [0 0 -0.9 0 0; 0 -0.9 -1.9 -0.9 0; -0.9 -1.9 16 -1.9 -0.9; 0 -0.9 -1.9 -0.9 0; 0 0 -0.9 0 0];
s = im2double (fr3);
g2 = imfilter (s, w, 'replicate');
imshow (g2, [])
g3 = s + g2;
title ('Podcherkivanie graniz vosstanovlennogo izobrajeniya');
gs5 = im2uint8 (mat2gray (g3));
```

5. Пороговая бинаризация по методу Отса:

```
T = graythresh (g3);
```

6. Морфологическая фильтриция бинарного изображения.

6.1. Дилатация и удаление изолированных пикселей переднего плана:

```
g = im2bw (g3, T);
```

6.2. Создание структурообразующего элемента:

```
B = [0 1 0; 1 1 1; 0 1 0];
Izobr = imdilate (g, B);
Imshow (izobr);
```

6.3. Заполнение однопиксельных «дырок» (рисунок 2):

```
izobr1 = bwmorph (izobr, 'clean', Inf);
izobr2 = bwmorph (izobr1, 'fill', Inf);
```

Рисунок 2. Результат заполнения однопиксельных «дырок»

7. Поиск объектов на изображении путем вычисления связных компонентов. Определение площади объектов изображения:

```
[L, n] = bwlabel (izobr2);
sumpixeles = zeros (1,36);
 for k = 0:35
 se = strel ('disk', k);
 fo = imopen (g, se);
 sumpixels (k + 1) = sum (fo(:));
end
```

8. Построение распределения крупности частиц (гранулометрического состава руды):

```
plot (logncdf (0:300,sumpixels(k+1)))
xlabel ('size diametr [mm]')
ylabel ('the number of particles in the image[pcs]')
```

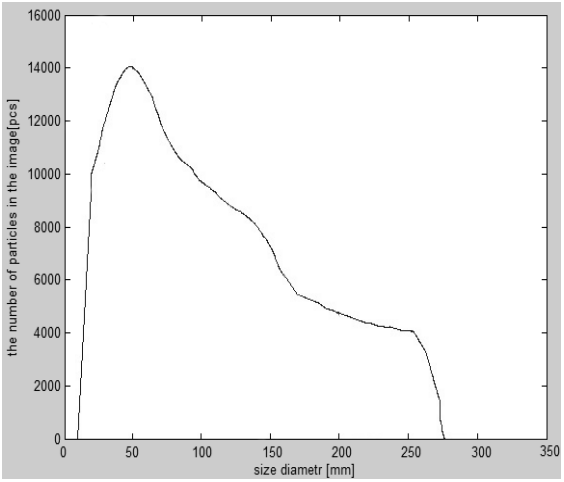


Рисунок 8. График гранулометрического состава руды

ВЫВОДЫ

1. Установлено, что на этапе формирования изображения предпочтительным является фильтр Винера с использованием автокорреляционных функций.

2. Для формирования бинарного изображения операция подчеркивания границ и пороговая бинаризация имеет преимущества перед градиентными методами Собеля или лапласиана гауссиана.

3. Морфологическая фильтрация позволила устранить бинарные помехи на изображении и определить гранулометрический состав частиц с относительной ошибкой не более 5%.

СПИСОК ЛИТЕРАТУРЫ

1. Корнієнко В.І. Логічні алгоритми обробки бінарних зображень в оптичному гранулометрі дроблених матеріалів// Науковий вісник Національного гірничого університету. – 2006. – № 11. – С. 89-90

2. «Цифровая обработка изображений в информационных системах» Учеб. пособие/ И.С Грузман, В.С.Киричук и др.-Новосибирск: Изд-во НГТУ,2002-352с.

3. «Цифровая обработка изображений. изображений в среде MATLAB» Р.Гонсалес, Р.Вудс. Перевод с английского под редакцией П.А.Чочиа. Москва: Издательство «Техносфера», 2006.-616с.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

VII ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

26 березня 2015 р.

Підписано до друку 16.03.15. Формат 30 х 42/2.
Папір офсетний. Ризографія. Ум.друк.арк. 9,6
Обл.-вид.арк. 9,4. Тираж 50 прим. Зам. № __

Підготовлено до друку у Державному ВНЗ
«Національний гірничий університет»
49005, м. Дніпропетровськ, просп. К. Маркса, 19

Надруковано у ТОВ «САЛВЕЙ»
Свідоцтво № 233689904636
49000, м. Дніпропетровськ, вул. ак. Чекмарьова, 10 / 7