Управління розвитком

Харківський національний економічний університет

І міжнародна науково-практична конференція "Безпека та захист інформації в інформаційних і телекомунікаційних системах"

Секція 1 "Методи та технології безпеки інформаційних систем"

Секція 2 "Захист інформації в комп'ютерних системах"

Секція 3 "Інформаційні та телекомунікаційні системи в бізнесі"

28 – 29 травня 2008 року

Збірник наукових статей

видається 2 рази на рік

№6'2008

Харків. Вид. ХНЕУ, 2008

ЗБІРНИК НАУКОВИХ СТАТЕЙ

Управління РОЗВИТКОМ №6'2008

Засновник і видавець

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Реєстраційний номер свідоцтва КВ №5948 від 19 березня 2002 р.
Затверджено на засіданні вченої ради університету.
Протокол №9 від 21.04.2008 р.

Редакційна колегія

Редакція збірника наукових статей

Зав. редакції ***Сєдова Л. М.***
Редактори: ***Лященко Т. О.***
Нещеретна О. М.
Голінська О. Г.
Грицай І. М.
Дуднік О. М.
Замазій О. Є.
Комп'ютерна верстка ***Климович Т. М.***

Адреса видавця: *61001, Україна, м. Харків, пр. Леніна, 9а*
Телефони:
(057)702-03-04 — головний редактор
(057)758-77-05 — зав. редакції
E-mail: *vydav@ksue.edu.ua*

Відповідальність за достовірність фактів, дат, назв, імен, прізвищ, цифрових даних, які наводяться, несуть автори статей.
Рішення про публікацію статті приймає редакційна колегія. У текст статті без узгодження з автором можуть бути внесені редакційні виправлення або скорочення.
Редакція залишає за собою право їх опублікування у вигляді коротких повідомлень і рефератів.

При передрукуванні матеріалів посилання на збірник обов'язкове.

Підписано до друку 21.04.2008 р.
Формат 84×108 1/16. Папір MultiCopy.
Ум.-друк. арк. 19,0. Обл.-вид. арк. 23,75. Тираж 500 прим. Зам. № 282.
Ціна договірна.

Надруковано з оригінал-макета на Riso-6300 61001, м. Харків, пр. Леніна, 9а.
Видавництво ХНЕУ.

Секція 1
Методи та технології безпеки інформаційних систем

УДК 351.861

Альбощій О. В.

Попов В.М.

УПРАВЛІННЯ РИЗИКАМИ ЯК МЕТОДОЛОГІЧНА ОСНОВА ДІЯЛЬНОСТІ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Незважаючи на зусилля щодо забезпечення належного рівня техногенної та природної безпеки, зокрема удосконалення структури єдиної системи цивільного захисту, розбудову Оперативно-рятувальної служби цивільного захисту та інших сил реагування, даний рівень безпеки в Україні залишається низьким та має тенденцію до погіршення. Серед кола причин такого стану є й методологічні, які стосуються концептуальных основ діяльності у сфері цивільного захисту. Досвід зарубіжних країн свідчить, що в сучасних умовах необхідно переходити на принципово іншу основу державної політики у сфері захисту населення й територій від надзвичайних ситуацій техногенного та природного характеру, яка ґрунтується на концепції управління ризиками.

Загальні положення теорії управління ризиками та їх основні прикладні аспекти стосовно сфери цивільного захисту можна знайти в роботах [1 – 4].

Серед пріоритетних завдань МНС на 2008 рік визначено здійснення превентивних заходів щодо запобігання надзвичайним ситуаціям [5]. Це відповідає сучасним поглядам на функціонування національних систем цивільного захисту розвинених країн. Виходячи з доцільності впровадження в практику концепції управління ризиками, визначимо ключові методологічні аспекти, які мають бути покладеними в основу захисту населення від надзвичайних ситуацій техногенного та природного характеру.

Надзвичайна ситуація – це порушення нормальних умов життя й діяльності людей на об'єкті або території, спричинене аварією, катастрофою, стихійним лихом, епідемією, епізоотією, епіфітотією, великою пожежею, застосуванням засобів ураження, що призвели або можуть призвести до людських і матеріальних втрат [1]. Причини надзвичайних ситуацій можуть бути різного походження. Якщо не приймати до розгляду можливість цілеспрямованого впливу суб'єктивного характеру, то кожну конкретну причину можна представити як наслідок випадкового збігу факторів, в результаті якого один чи більше параметрів процесу перевищили критичні межі, чим обумовили неконтрольований розвиток процесу.

Динамічний і незворотний характер розвитку надзвичайних ситуацій, велика швидкість протікання процесів потребують якомога швидкого втручання, локалізації та ліквідації наслідків. Оперативне реагування є реакцією на випадкові події, що сталися. У той же час виникає питання, "а чи можливо було передбачити подібні випадкові події й втрутитись у процеси до того, як їх параметри досягли критичної межі?". Така постановка питання відповідає методології превентивної діяльності, теоретичним підґрунтям якої може бути теорія управління ризиками.

Ризик – це можлива загроза від будь-якого несприятливого результату [1]. Ризик у широкому розумінні – характеристика ситуації, для якої властива невизначеність результату при обов'язковій наявності небажаних наслідків. Під управлінням ризиком у сфері цивільного захисту будемо розуміти цілеспрямований вплив на об'єкт (процес) з метою недопущення надзвичайної ситуації або пом'якшення її можливих наслідків. Тоді основним завданням процесу управління ризиками слід вважати зниження ймовірності виникнення надзвичайних ситуацій шляхом своєчасного виявлення негативних тенденцій у розвитку процесів та відповідного впливу на суттєві параметри. У той же час важливим завдання є зниження рівня можливих негативних наслідків.

Реалізація концепції управління ризиками можлива лише на системних засадах. Центральне місце в такій системі відводиться інформаційній складовій. Спираючись на зарубіжний досвід [2] можна вважати, що до основних функціональних підсистем інформаційного блоку відносяться:

1. Геоінформаційна підсистема. Її основне призначення – накопичення інформації про території та об'єкти, які на них знаходяться. Така інформація повинна бути у вигляді електронних карт території, міст, планів окремих районів і підприємств.

---

2. Підсистема зберігання даних. Призначена для накопичення та зберігання бази даних про потенційно небезпечні об'єкти, системи життєзабезпечення; сили і засоби для ліквідації надзвичайних ситуацій.

3. Підсистема моніторингу. Призначена для оперативного прийому, обробки, зберігання й видачі споживачам інформації. У рамках даної підсистеми проводиться виявлення негативних тенденцій, викликаних тими чи іншими факторами, моніторинг і патрулювання пожежної обстановки, оцінка ступеня забруднення природних комплексів; оцінка й виявлення проривів трубопроводів, уточнення місць розташування й характеристик екологічно небезпечних об'єктів, контроль паводкової ситуації та ін.

4. Підсистема аналітичної обробки даних. Її призначення – моделювання надзвичайних ситуацій і планування заходів щодо їх попередження та ліквідації, забезпечення інформаційної підтримки оперативних заходів щодо ліквідації наслідків надзвичайних ситуацій, ранжування об'єктів і територій за показниками небезпеки.

Відправним пунктом управління ризиками є оцінювання ризиків. Якісне оцінювання передбачає виявленням існуючих ризиків, їх фіксацію. Залежно від об'єкта, що розглядається, кількість ризиків може суттєво змінюватись. Більш того, по відношенню до конкретного об'єкта не завжди можна передбачити всі можливі ризики. За таких умов доцільно встановити найбільш суттєві з них, а також ті процеси, які найбільшою мірою піддані їх впливу. Кількісне оцінювання виявлених ризиків передбачає отримання оцінок показників ризику. У загальному випадку ризик є векторною величиною, яка включає такі показники:

величина збитку від впливу того чи іншого небезпечного фактора;

ймовірність (частота) виникнення фактора, що розглядається;

невизначеність у значеннях збитку та ймовірності.

Стосовно надзвичайних ситуацій техногенного та природного характеру отримати кількісні оцінки даних показників можливо або на основі статистичних даних або за результатами математичного моделювання. Статистичні методи дають змогу виявити закономірності в таких масових явищах як надзвичайні ситуації й розрахувати середньостатистичне значення збитку та ймовірність (частоту) настання надзвичайних ситуацій за різними видами. Математичне моделювання дозволяє спрогнозувати розвиток надзвичайної ситуації конкретного виду з урахуванням її випадкового характеру, оцінити наслідки (збитки) при заданих вхідних параметрах.

Після визначення рівня ризику конкретного виду передбачається розробка варіантів управлінського впливу та конкретних заходів.

Залежно від рівня ризику та реальних можливостей щодо впливу на ситуацію заходи управління ризиками можуть спрямовуватися за декількома напрямками. Можливі способи обробки ризиків за умови, що прийнято три рівні градації ризику, подані на рисунку.

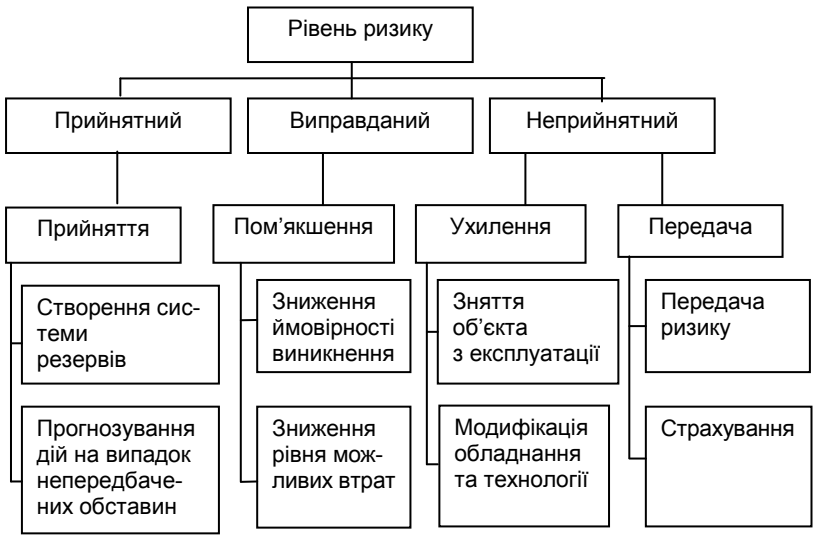


Рис. **Загальна характеристика способів обробки ризиків**

Наведені способи обробки ризиків відповідають основним завданням управління ризиками та можуть бути покладені в основу роботи щодо реалізації на практиці концепції управління ризиками у сфері цивільного захисту.

Отже, одним із важливих шляхів підвищення рівня техногенної та природної безпеки є удосконалення методологічної основи діяльності у сфері цивільного захисту, приведення її до потреб часу. Зарубіжний досвід вказує на доцільність запровадження концепції управління ризиками та проведення на її основі превентивних заходів.

Запровадження концепції управління ризиками пов'язано із створенням функціональних підсистем, організацією їх роботи та налагодженням зв'язків між ними. Відправною точкою є оцінювання ризиків з наступною розробкою заходів впливу на суттєві фактори.

Література: 1. Лазарєв А. А. Менеджмент страхування та ризику: Навч. посіб. – Харків: Акад. ВВ МВС України, 2006. – 70 с. 2. Ямалов И. У. Комплексная оценка рисков – основа обеспечения защиты населения и территории от чрезвычайных ситуаций // www. meteoagency. ru/sgmo/merop_sgmo/ufa/11.doc 3. Гражданкин А. И. Основные показатели риска аварии в терминах теории вероятностей / А. И. Гражданкин, Д. В. Дегтярев, М. В. Лисанов, А. С. Печеркин //Безопасность труда в промышленности. – 2002. – №7. – С. 35 – 39. 4. Вокарев А. А. Вопросы прогнозирования последствий чрезвычайных ситуаций в экономике региона. МОУ "Волжский институт экономики, педагогики и права // www. rusnauka. com/PRNIT_2006/ Economics/ 16542.doc. htm 5. Рішення Колегії МНС від 17.01.2008 р. "Про результати роботи Міністерства у 2007 році та пріоритетні завдання на 2008 рік" // www.rada.gov.ua

УДК 65.012.8

Акімов В. В.

Назаренко Д. В.

ЗАГАЛЬНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

Не випадково особливістю нашого часу називають перехід від індустріального суспільства до інформаційного, в якому головним ресурсом стає не капітал, а інформація. Тому в організації безпеки підприємства домінуючого значення набуває захист інформації. Сьогодні для перемоги в конкурентній боротьбі підприємства необхідна не озброєність працею, ресурсами, капіталом, а озброєність знаннями, інформацією. Отже, інформаційна безпека передбачає визначення секретів і комерційної таємниці, організацію комунікаційних процесів у підприємства, які б виключали можливість їх витікання. Фахівці вважають [1], що втрата 20% комерційної таємниці підприємства підвищує коефіцієнт його можливого банкрутства до 0,6. Тому захист комерційної таємниці є складовою частиною інформаційної безпеки взагалі. Але його особливість полягає в тому, що предмет безпеки, методи її забезпечення в межах чинного законодавства визначаються суб'єктом господарювання. Усе це обумовило особливу актуальність з питань практичного захисту інформації і проблему забезпечення економічної безпеки українських підприємств.

Питанням економічної безпеки суб'єктів господарювання присвячені роботи таких вітчизняних вчених: В. С. Пономаренка, М. В. Куркіна, В. І. Мунтіяна, В. М. Гейця, В. Є. Духова, М. О. Кизима, В. Д. Понікарова та ін. Але, незважаючи на значну кількість наукових праць, є достатня кількість невирішених проблем.

Мета статті полягає в глибокому та всебічному розгляді загальних методологічних підходів до захисту інформації та методів підвищення економічної безпеки підприємства.

У сучасних умовах високих темпів інформаційного прогресу в суспільстві інформаційна безпека посідає особливо важливе місце в системі економічної безпеки підприємства. Отже, інформаційна безпека заснована не тільки на захисті власної інформації, в тому числі конфіденційної, але й проводить ділову розвідку, інформаційно-аналітичну роботу із зовнішніми і внутрішніми суб'єктами тощо [2].

Саме стаття 9 Закону України "Про інформацію" [3] визначає право на інформацію, тобто всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи й законні інтереси інших громадян, права та інтереси юридичних осіб. Тому сьогодні однією з головних актуальних проблем економічної безпеки України є проблеми захисту інформації в системі економічної безпеки суб'єкта господарювання.

Поняття інформації, просте на перший погляд, має дуже складний зміст, відмінний від звичайного уявлення про інформацію як відомості, що переказуються, а також процес переказу до філософської категорії, за допомогою якої відображаються реалії світу. Для цілей формування інфор-

маційної безпеки визначимо інформацію як сингали, що циркулюють в системі і поміж системами й використовуються ними для власного розвитку.

В економічному сенсі інформація – це відомості про наявність ресурсів, капіталу та інших факторів виробництва, технологій, обсяги виробництва продуктів і послуг, витрат, доходів, взаємних угод тощо. Інформація має велику кількість властивостей, але з точки зору її безпеки цікаві декілька: здатність запам'ятовуватися, фіксуватись і зберігатись. Завдяки ним є можливість відокремлювати в часі й просторі моменти виникнення інформації та її використання. Але ж разом з тим є можливість несанкціонованого доступу й використання інформації [4].

У результаті, наприклад, питання захисту комерційної таємниці нерідко випускаються в ліцензійних угодах, договорах підряду на створення науково-технічної продукції, що призводить до витоку комерційної інформації.

Заходи забезпечення збереження інформації на окремому підприємстві можуть бути різні за масштабами і формами й залежати від виробничих, фінансових та інших можливостей підприємства, від кількості і якості комерційних таємниць, які охороняються. При цьому вибір таких заходів необхідно здійснювати, виходячи з принципу їх розумної достатності, дотримуючись у фінансових розрахунках "золотої середини", оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, може викликати втрату певної частки прибутку або призвести до серйозних збитків [3].

Визначаючи, що зберігання інформації є одним із важливих аспектів економічної безпеки діяльності підприємства, необхідно відзначити, що зведення економічної безпеки підприємства тільки до захисту комерційної таємниці не враховує всього спектра впливу зовнішнього середовища як основного джерела небезпек для діяльності підприємства. У зв'язку з цим економічна безпека повинна розглядатися як можливість забезпечення його стійкості в різноманітних умовах, у тому числі й у несприятливих, що полягають у зовнішньому середовищі незалежно від характеру його впливу на діяльність підприємства, масштабу і характеру внутрішніх змін [2].

У літературі з економічної безпеки висвітлена значна кількість питань практичного захисту інформації. В даному випадку буде розглянуто загальні методологічні підходи до захисту інформації взагалі. Ключовими питаннями захисту інформації є проблеми впорядкованості інформаційної системи, доступу до інформаційної системи, безпеки інформаційної системи, контролю й сумісності безпеки інформаційної системи із загальною безпекою суб'єкта господарювання.

Розглянемо ці проблеми у певній послідовності.

Першим кроком на шляху до формування безпечної інформаційної системи є її впорядкованість. Головний принцип, який варто неухильно підтримувати, – це військове положення: кожен має отримувати ту інформацію і в такому обсязі, що потрібно для ефективного виконання роботи. Але надмірна інформація незалежно від її цінності частіше втрачається. Необхідно також пам'ятати, що без упорядкування інформаційної системи всі інші засоби її захисту є безглуздими.

Після впорядкування інформаційної системи наступним кроком її захисту є блокування несанкціонованого доступу. Ця проблема вирішується в декількох напрямках роботи. Передусім контролюються процеси формування, проходження й використання інформації. Це здійснюється традиційними і сучасними технічними засобами: від журнального обліку, що здійснюють канцелярії, до комп'ютерного протоколювання.

Наступним послідовним кроком здійснення захисту інформації є забезпечення її безпеки. Вона визначається наступними рисами:

1) відсутністю порушень таємності інформації;

2) відсутністю порушень цілісності інформації.

Тому загальним завданням безпеки секретної інформації є блокування доступу до неї, блокування спроб порушення цілісності інформації, поновлення таємності та цілісності. Можна вважати, що ці чотири фактори є теоретичними обмеженнями системи безпеки інформації.

Ефективне вирішення попередніх проблем, як будь-яке інше рішення в менеджменті, потребує відповідного контролю. Завдання контролю вирішується одночасно з вирішенням проблеми доступу до конфіденційної інформації.

Завданням контролю є недопущення і виявлення порушень безпеки інформаційної системи фірми, яка можлива тільки в процесі обміну інформацією, коли вона починає циркулювати в системі, тобто в процесі обміну між джерелами та адресатами. Також контроль повинен бути спрямований на блокування доступу до тієї інформації, яка зберігається або вилучається з інформаційної системи взагалі. Йдеться про інформацію, що не підлягає зберіганню, але може мати економічну, соціальну чи політичну цінність. Не менше уваги в процесі здійснення контролю треба надавати її знищенню, щоб вона не потрапила до конкурента, якщо в цьому немає необхідності [6].

Вирішення всіх перелічених вище проблем безпеки інформаційної системи фірми здійснюється комплексно в системі загальної економічної безпеки. У зв'язку з цим можна визначити декілька аспектів.

Передусім це проблема взаємодії технічного та людського чинників. Якщо коефіцієнт упорядкованості технічних засобів захисту може дорівнювати одиниці, то коефіцієнт упорядкованості людського чинника внаслідок його суспільної природи, ніколи не дорівнює одиниці. Чим нижче дисципліна в колективі, тим нижче коефіцієнт упорядкованості цього чинника безпеки, тим більше проблем із захисту інформації. Технічній фактор має визначальне значення в протидії технічним засобам збирання інформації конкурентами, злочинцями тощо. Але й працівник у власних інтересах може приховувати факти порушення системи інформації.

Інший аспект − це узгодженість алгоритму функціонування системи інформаційної безпеки із системою економічної безпеки підприємства в цілому. Незалежно від організаційного рівня захисту інформаційної системи підприємства, якщо інші складові економічної безпеки мають суттєві вади, втрати інформації будуть мати місце.

Наступний аспект − це узгодженість алгоритму захисту інформації з правовими нормами та алгоритмом захисту державних секретів [4].

Слід зазначити, що ефективність політики безпеки тільки тоді знаходитиметься на належному рівні, коли її реалізація буде результатом спільної діяльності співробітників організації, здатних зрозуміти всі її аспекти, і керівників, здатних впливати на її втілення в життя. Роботи щодо оснащення й підтримки діяльності системи захисту інформації, створення системи розпорядчих документів входять у комплекс організаційних заходів, на основі якого може бути досягнутий високий рівень безпеки інформації. Проте перераховані заходи не дозволяють на належному рівні підтримувати функціонування системи захисту без проведення цілої низки організаційно-технічних заходів. Тому, як і будь-яка кваліфікована робота, вимагає участі в ній фахівців, які мають відповідну професійну підготовку, а також володіють практичним досвідом.

Література: 1. Бандурка О. М. Основи економічної безпеки: Підручник / О. М. Бандурка, В. Є. Духов, К. Я. Петрова, І. М. Червяков. – Харків: Вид. Нац. ун-ту внутр. справ, 2003. – 236 с. 2. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство. Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк; [За ред. В. М. Гейця. – Харків: ВД "ІНЖЕК", 2006. – 240 с. 3. Закон України "Про інформацію" // Відомості Верховної Ради. – 1992. – №48. – Ст. 650. 4. Орлов П. І. Основи економічної безпеки фірми: Навчальний посібник / П. І. Орлов, В. Є. Духов. – Харків: ТОВ "Прометей-Прес", 2004. – 284 с. 5. Економічна безпека держави: стан, проблеми, напрями зміцнення // Матеріали Наук.-практ. конф. Харків, 27 жовтня 2006 р. – Харків: ХНУВС, 2007. – 278 с. 6. Куркін М. В. Ревізії та перевірки за зверненнями правоохоронних органів. Навчальний посібник / М. В. Куркін, В. Д. Понікаров. – Харків: Східно-регіональний центр гуманітарно-освітніх ініціатив, 2003. – 412 с.

УДК 004.78:338.78

Кавун С. В.

Сорбат И. В.

ИНСАЙДЕР – УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В настоящее время значительная часть предпринимателей различного уровня понимают, что информация является товаром и орудием борьбы. Сегодня забота обеспечения экономической безопасности (ЭБ) бизнеса − насущная проблема любого предпринимателя.

Современный мир бизнеса, как известно, очень сильно связан с информационными технологиями (ИТ), а следовательно, индустрия информационной безопасности (ИБ), обороты которой составляют не один миллиард долларов, имеет ключевое значение в успешном развитии и процветании отдельных участников того или иного рынка, а следовательно, экономики страны в целом. Наиболее опасной внутренней угрозой для компании являются инсайдеры. Инсайдер − пользователь информационной системы, имеющий вполне легальный доступ к конфиденциальной информации и применяющий весь арсенал доступных ему средств для того, чтобы использовать конфиденциальную информацию в своих интересах.

Утечку информации через инсайдеров трудно предугадать и предотвратить, а значит, для борьбы с ними службе безопасности необходимо задействовать весь арсенал доступных комплексных мер и средств. Умышленная или нет деятельность инсайдеров в большинстве случаев приводит к убыткам и потере прибыли. Наибольшую опасность феномен инсайдерства представляет для крупного бизнеса, чем больше сфера влияний той или иной корпорации, тем важнее для её работы и успеха информационные активы [1].

Вопросы защиты и сохранности информации, конечно, давно и внимательно изучаются теми, кто создает коммерческие программы. Проблема, однако, в том, что сами руководители компаний зачастую не слишком задумываются над тем, кто и каким объемом информации должен владеть. Нередки случаи, когда даже тот набор средств, который заложен в коммерческую программу, не используется по назначению. Мало внимания уделяется таким аспектам, как доступ к информации сотрудников различных уровней. Инсайдеры представляют угрозу, прежде всего, для интеллектуальной собственности организации − одного из ее основных активов. Установление и

защита прав на интеллектуальную собственность в настоящее время является важнейшим аспектом любого бизнеса, в особенности малого, являющегося, как известно, оплотом любой здоровой экономики.

Исследования "2006 Global Security Survey" показало, что основными приоритетами современных финансовых компаний являются совместимость с международными нормативными актами (67%), защита от кражи личности и мошенничества со счетами (58%), непрерывность бизнеса (49%), улучшение инфраструктуры (41%) и управление идентификацией (41%). Таким образом, вектор развития ИБ в финансовых компаниях указывает по направлению совместимости со стандартами и внутренней ИБ.

В 2007 году 72% финансовых компаний, которые пострадали от утечки информации, оценили свои прямые и косвенные убытки в районе 1 млн долл., а у 2% респондентов ущерб превысил 5 млн долл. При этом 69% компаний провели классификацию своих информационных активов, чтобы отделить конфиденциальные документы фирмы и приватные сведения клиентов от публичных данных. Можно резюмировать, что банки и страховые компании сегодня, как никогда ранее, чувствительны к утечке важной информации.

Исследования компанией Deloitte показало, что 80% крупнейших кредитно-финансовых организаций мира используют мониторинг действий инсайдеров. Это наиболее эффективная мера, которую бизнес может принять, чтобы предотвратить утечку конфиденциальной информации, заблаговременно выявить мошенничество, защититься от саботажа или злоупотребления корпоративными ресурсами. К сожалению, в Украине этот процент намного меньше. Отечественные компании, в том числе банки и страховые компании, практически не пользуются средствами мониторинга [2].

Из результатов исследований, проведенных аналитическим центром компании Perimetrix, были выделены основные проблемы ИБ, приводящие к угрозе ЭБ в целом. Устаревшие системы, внедрявшиеся в начале века, уже не достаточно эффективно противостоят нарушителям, потому что изменился сам характер угроз. К примеру, раньше инсайдеры чаще всего использовали сетевые службы (электронную почту, Интернет и пр.), а сейчас просто копируют нужные документы на USB-носители и уносят их в кармане. Помимо этого, участились и случаи халатных утечек. Лояльные работники выносят с работы те же USB-накопители или ноутбуки, а затем теряют технику и всю конфиденциальную информацию вместе с ней. Кроме того, подразделениям ИБ не хватает квалифицированных кадров, особенно для борьбы с внутренними нарушителями. Также имеются определенные трудности с внедрением новых продуктов безопасности в существующие информационные системы.

Компания Perimetrix с 10 января по 10 февраля 2008 года провела опрос сотрудников 472 российских организаций. Респонденты отвечали на вопросы по электронной почте, в телефонных беседах, при личном интервью в своем офисе, а также заполняли online-анкеты на сайте SecurityLab. Выборка респондентов имеет уклон в сторону крупных и средних компаний. Предприятия малого бизнеса (менее 500 работников) малочисленны и составляют всего 4% респондентов. Чем крупнее организация, тем больший урон наносят утечки. Ведь крупные участники рынка в большей степени страдают от ухудшения репутации, когда становится известно об инциденте. Поэтому и в исследовании преобладают компании среднего (от 500 до 2,5 тыс. работников, 54% участников) и крупного (свыше 2,5 тыс. работников, 42%) бизнеса [3].

Уровень компьютеризации участвовавших в опросе организаций очень высок. Компании до 500 рабочих станций составляют те же 4%, что и участники малого бизнеса. Доля фирм от 500 до 1 тыс. компьютеров значительно больше и равняется 40%. Почти столько же (37%) приходится на организации и учреждения от 1 тыс. до 5 тыс. рабочих станций.

Что касается сферы деятельности компаний, лидерами являются сектор финансовых услуг (26%), ИТ и телекоммуникации (21%), а также ТЭК (19%). Немногим меньше (14%) приходится на различные государственные учреждения, министерства и ведомства. Фирмы-производители, предприятия торговли и страховые компании имеют долю от 7% до 4%, всего 2% – образовательные учреждения, 1% фирм не относится ни к одной из перечисленных сфер.

Среди респондентов исследования работники ИТ и ИБ составляют примерно равные группы с преобладанием руководящего состава. 53% сотрудников ИТ включают 48% начальников отделов и 5% служащих. В свою очередь 47% работников подразделений ИБ составляют 36% руководителей отделов и 11% специалистов. Таким образом, результаты исследования строятся с учетом мнений людей, которые определяют развитие систем ИБ в организациях.

Один из основных вопросов, заданных респондентам, касается угроз ИБ, а следовательно и ЭБ. Участники исследования могли выбрать четыре различных фактора риска. Наибольшие опасения специалистов вызывают утечки данных (76%) и халатность пользователей (67%).

Следующий набор вопросов, которые касаются внутренних угроз ИБ, представлено на рис. 1 [3]. На каждый вопрос респонденты могли указать по 2 ответа. Наиболее опасную внутреннюю угрозу представляет опять же утечка данных (корпоративных секретов, интеллектуальной собственности и пр.). Этот фактор выбрала почти половина специалистов (46%). Близкие по смыслу угрозы, искажение документации и утрата информации, набрали соответственно 37% и 31%. Чуть менее опасны, по мнению ИБ и ИТ-специалистов, сбои в работе информационных систем (ИС) – 26% и саботаж – 22%. 20% в пункте кража оборудования говорит о том, что собственные сотрудники воруют технические устройства значительно меньше, чем информацию. Вынести электронный файл легче и прибыльнее, чем, к примеру, сетевое оборудование.

Рис. 1. **Самые опасные угрозы внутренней ИБ ИС**

Что же чаще всего утекает из организаций? Можно предположить, что интеллектуальная собственность и корпоративные секреты. Оказывается, не совсем так (рис. 2). Еще чаще (57%) крадут персональные данные. Это тоже не удивительно. В последние годы известно немало случаев, когда крупные утечки персональных данных клиентов случались в отечественных банках. В скандальных новостях оказались замешаны даже гиганты кредитной сферы, а также известные игроки на рынке телекоммуникационных услуг. Вслед за персональными данными действительно идут детали конкретных сделок (47%), финансовые отчеты (38%) и интеллектуальная собственность (25%). Бизнес-планы набрали 19%, а прочие информационные ресурсы – 14%.

Рис. 2. **Информация, наиболее подверженная утечке**

Отвечая на вопрос о наиболее опасных угрозах ИБ, респонденты данного исследования поставили на первое место утечки и халатность служащих. При этом атаки хакеров и вирусная активность заметно отстали. Кроме того, 98% компаний применяют контроль доступа, 74% – системы обнаружения/предотвращения вторжений (IDS/IPS) и 53% – VPN-соединения. Данные меры также снижают шансы хакеров и вредоносного кода на успех. Получается, от внешних угроз защищают сразу несколько различных технологий, но в то же время организации оказываются беззащитными перед столь актуальными внутренними угрозами. Ведь только 36% компаний шифруют данные при хранении, а системами защиты от утечек оснащены и того меньше, 24% фирм.

Необходимо отметить, что участники исследования не были ограничены в количестве ответов на вопросы о мерах защиты, то есть были перечислены все имеющиеся в компаниях средства. Почему же уровень использования средств защиты от утечек столь низок? Специалисты называют множество причин. Самый популярный ответ – неэффективность предлагаемых технологий (49%). Далее идут традиционные бюджетные ограничения (26%) и трудности с внедрением (11%) [3].

Если проанализировать ответы специалистов, принявших участие в исследовании, станет ясно, что ситуация в сфере ИБ неудовлетворительная. Особенно в части утечек данных. Тем не менее, респонденты решительно настроены укреплять ЭБ, но каждый по-своему. Ответы на последний вопрос наглядно демонстрируют, в каком направлении организации собираются развивать отрасль ИБ в ближайшее время. Сотрудники отделов ИТ и ИБ могли бы перечислить многие мероприятия. Поэтому, чтобы выявить наиболее важные направления, количество вариантов ответа было ограничено всего одним.

Нет ничего удивительного, что большая часть специалистов (34%) рассчитывает укрепить защиту от утечек. Это просто необходимо, ведь инсайдеры представляют наиболее опасную угрозу. На втором месте с 22% идет шифрование данных – тоже весьма эффективное мероприятие от потери информации. Чуть меньше (19%) набрали комплексные инструменты ИБ – IDS/IPS. В 15%

компаний планируют улучшить системы резервного копирования. А 10% респондентов назвали другие компоненты.

Результаты исследования показали, что, несмотря на позитивное отношение специалистов к техническим средствам защиты от утечек в "теории", на практике эти решения внедрены лишь в нескольких наиболее крупных фирмах. А те, что используют, применяют, в основном, устаревшие малоэффективные комплексы, которые основываются на методах контентной фильтрации. Недооцененными остаются такие технологии, как шифрование хранимых данных и классификация.

Согласно подсчетам аналитического центра Perimetrix, финансовый ущерб от потери персональных данных всего 1 человека обходится примерно в 200 долл., а крупные компании теряют базы данных клиентов по несколько миллионов записей. Тогда счет убытками идет уже на миллиарды. Неудивительно, что специалисты и руководители отделов ИТ и ИБ называют утечки самой большой угрозой ЭБ.

Следует отметить положительную тенденцию. Организации знают о существующих брешах в системах безопасности и намерены решительно с ними бороться [4].

Таким образом, проблемы внутренней ИБ – защиты от утечек и инсайдеров – по-прежнему возглавляют список приоритетных задач, которые компаниям придется решать в течение ближайшего года [5].

Целью статьи является акцентирование внимания руководителей различного ранга на деятельность инсайдеров в организации, с созданием рекомендаций противодействия инсайдерской угрозе ЭБ на техническом и организационном уровнях.

Информация утекает с использованием различных средств, способных эту самую информацию тем или иным способом запоминать.

Рекомендуются следующие варианты противодействия на техническом уровне:

физическое отключение всех интерфейсов (это USB-порты, дисковые устройства CD-ROM и floppy);

программное блокирование интерфейсов;

использование специализированного терминального ПО, которое будет работать с данными исключительно на сервере (на примере банковских систем); подавление сигналов.

Одним из возможных вариантов может быть контроль буфера обмена, что предотвратит сохранение информации методом □копировать – вставить□в какой-нибудь из документов, на которые у злоумышленника есть легальные права записи, копирования-распечатки.

Также на уровне инфокоммуникаций необходимо выполнить следующие рекомендации:

запретить использовать средства IM как таковые;

блокировать все сайты, кроме необходимых для работы;

включить мониторинг HTTP-трафика.

Технические решения не всегда эффективны в борьбе с инсайдерством, поэтому необходимо также применять организационные меры.

Рекомендуются следующие организационные меры:

создание политики безопасности компании;

многоуровневый доступ к информации;

постоянное, по возможности, повышение квалификации сотрудников безопасности;

регулярные брифинги для персонала;

аккуратность при приеме на работу новых кадров;

контроль вносимой и выносимой техники.

В политике безопасности, с которой каждый сотрудник в обязательном порядке должен ознакомиться, ясно и доходчиво должно быть изложено что можно, а что нельзя, и что практически вся информация не подлежит разглашению. Можно проинформировать сотрудников о последствиях утечки информации. С этой же целью можно использовать и регулярные брифинги, на которых до сотрудников будут донесены все изменения политик безопасности, если таковые были внесены. Но главной целью подобных мероприятий должно являться повышение сознательности и ответственности персонала.

Многоуровневый доступ к информации подразумевает, что вся информация, необходимая фирме в её работе, должна быть разбита на категории, которым, в свою очередь, должен быть присвоен определенный приоритет. На основе этого приоритета и должен осуществляться доступ, то есть, к примеру, бухгалтер не узнает то, к чему имеет доступ отдел программистов. И так далее по аналогии. Очевидно, что профилактика подобных инсайдерству инцидентов намного лучше, чем восстановление работоспособности и репутации. Поэтому совершенно необходимо очень внимательно присматриваться к новоприбывшим сотрудникам. Для этого можно содержать специально обученных людей, а можно обратиться к аутсорсинг-методам. Это означает, что все кандидаты для принятия на работу будут как бы процеживаться через фильтр специальных техник так называемого кадрового контроля, который включает в себя, помимо всех психологических тестов, проверку на детекторе лжи, и это еще больше повысит общую безопасность всей системы в целом.

Следовательно сделаем вывод, что внутренние факторы заметно опережают внешние в рейтинге угроз ИБ. Наибольшие опасения специалистов вызывают утечки данных и халатность сотрудников. Организации оснащены антивирусными программными обеспечениями и межсетевыми экранами, но лишь некоторые имеют защиту от утечек, поэтому данные утекают с угрожающей регулярностью. Чаще всего инсайдеры крадут из компаний персональные данные, детали конкретных

сделок и финансовые отчеты. Широко распространенные мобильные накопители, а также электронная почта являются самыми популярными каналами утечек. Исходя из проведенного анализа исследований угроз ЭБ, можно сказать, что перспективным направлением решения задач является модернизация существующих методик ИБ для борьбы с такой угрозой, как инсайдер.

Литература: 1. Кавун С. В. Информационная безопасность в бизнесе. – Харьков: Изд. ХНЕУ, 2007. – 408 с. 2. Исследования угроз ИБ Deloitte // www. deloitte.com 3. Отчет аналитического центра Perimetrix «Инсайдерские угрозы в России 2008» // http://perimetrix.ru/ 4. Защита от инсайдеров. Обзорный курс InfoWatch //http://www.pcmag.ru/elearning/course/index.php?COURSE_ID=7 5. Введение. Технические средства защиты //http://www.pcmag.ru/elearning/course/lesson.php? COURSE_ID=7&ID=34

УДК 681.3

Кобзев І. В.

Калякін С. В.

Горелов Ю. П.

ДО ПИТАННЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ БЕЗПЕЧНОГО ПРОВЕДЕННЯ ІСПИТІВ З ВИКОРИСТАННЯМ МЕРЕЖНИХ ЗАСОБІВ

Іспити за допомогою використання комп'ютерів проводяться з багатьох навчальних курсів. Під час іспиту студент використовує програмне середовище, різні види довідок, налагоджує отримані результати. Це дозволить викладачеві можливо об'єктивніше оцінити знання та уміння того, хто складає іспит. Такі іспити дозволяють підвищити мотивацію студентів і в основному використовуються при перевірці знань із програмування та комп'ютерного дизайну [1].

У більшій частині комп'ютерних класів, в яких проводяться іспити, є комп'ютерна мережа. Не можна допустити того, щоб під час іспиту студенти спілкувалися через мережу (чат) і могли спільно використовувати файли ("розшарені"). Найпростіше вирішення даної проблеми технічне – виключення концентратора (комутатора). Але це відразу створює ряд проблем: збір результатів іспиту, використання мережного програмного забезпечення, розподілених баз даних, робота з WEB-серверами і багато чого іншого.

Пропоноване програмне забезпечення дозволить вирішити ці проблеми. Основна ідея полягає в тому, що мережні комунікації будуть заблоковані, але студенти зможуть користуватися необхідними файлами, а результати іспитів завантажуватимуться на сервер через мережу. Пропонована система складається з двох частин. Серверна частина – на комп'ютері екзаменатора. Клієнтська частина – на комп'ютері того, хто складає іспит. Сервер управляє процедурою проходження іспиту, блокує процеси, завантажує й обробляє результати, виконані на машинах-клієнтах. Комп'ютер-клієнт отримує команди з сервера. Коли іспит розпочався, всі мережні застосування за винятком завантаження файлів на сервер стають непрацездатними. Кожен із тих, хто складає іспит тільки після введення імені/пароля має можливість завантажити результати виконання роботи на сервер. Ці файли зберігаються в окремих директоріях, і студент має доступ тільки у свою теку. Це дозволяє полегшити роботу екзаменаторові.

Основна мета полягає в тому, щоб розробити програмну систему для проведення іспитів з використанням комп'ютерів. Існуючі системи не дозволяють повністю вирішити проблему безпеки проведення таких іспитів і зокрема залишаються невирішеними питання збору й обробки результатів. Пропонована система повинна блокувати мережне спілкування між особами, що складають іспит і відправляти результати на сервер з метою подальшої їх обробки.

Система, що розробляється, повинна задовольняти наступним вимогам:

у комп'ютерів-клієнтів мережні комунікації повинні допускати блокування, щоб виключити з'єднання з сервером;

блокування може бути включено й зупинено командою із сервера;

комп'ютер-клієнт повинен отримувати пакети з сервера;

при перезавантаженні комп'ютера-клієнта управління ним із боку сервера не повинно перериватися;

на комп'ютері-клієнтові має бути інтерфейс для завантаження результатів іспиту на сервер;

студент повинен мати доступ до необхідного програмного забезпечення, використовуючи своє ім'я і пароль. Пароль надається після початку іспиту;

результати іспиту можуть зберігатися тільки в особистій теці студента на сервері;

екзаменаційні паролі повинні генеруватися для кожного студента окремо і зберігати в захищеній базі даних на сервері;

на сервері має вестися балка з історією роботи під час іспиту кожного комп'ютера-клієнта;

Система складається з двох частин: серверної та клієнтської. Клієнтська частина має три складових: сервіс клієнта, брандмауер і призначений для користувача інтерфейс (рисунок).

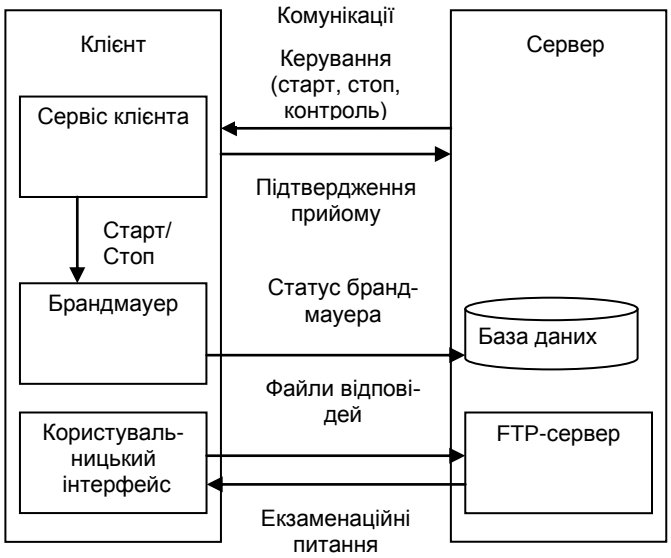


Рис. **Зв'язок між клієнтською та серверною частинами**

Клієнтська частина системи включається автоматично при завантаженні операційної системи. Брандмауер включений. Відбувається з'єднання і обмін службовою інформацією з сервером через дозволені й відкриті порти. Студент як FTP-клієнт отримує своє ім'я і пароль. Використовуючи дану інформацію, він може продивлятися свої питання і завантажувати на сервер в свої директорії файли відповідей.

У базі даних на сервері зберігаються номери задіяних комп'ютерних класів, IP-адреси комп'ютерів, списки осіб, які проходять іспит, їх питання і відповіді.

Алгоритм проведення іспиту наступний:

екзаменатор на екрані монітора бачить всі комп'ютери, підключені до сервера і на яких в даний момент проходить іспит;

за протоколом через 5888 порт кожні 3 секунди посилається широкомовне повідомлення □Контроль□;

порт 5889 служить для прийому пакетів від комп'ютерів-клієнтів;

система приймає повідомлення і відзначає ті комп'ютери, які в даний момент знаходяться в режимі “on-line”;

після початку іспиту включається FTP-сервер. UDP-пакет ”Start” безперервно посилається за всіма IP-адресами;

порт 5889 безперервно прослуховується на предмет отримання пакетів від комп'ютерів-клієнтів;

кожні 30 секунд порти 5892 і 3022 приймають пакети від брандмауера. Якщо пакет прийшов через порт 5892 на дисплеї відображається час відгуку. Отримання пакету через порт 3022 означає некоректну роботу брандмауера;

після закінчення часу проведення іспиту за протоколом UDP за IP адресами комп'ютерів, задіяних в іспиті, розсилається повідомлення “Stop”.

Використання протоколу UDP пояснюється тим, що він швидший, ніж протокол TCP.

FTP-сервер запускається через порт 5890 і далі через порт 5891 відбувається обмін даними (файли питань і відповідей) між клієнтськими машинами і сервером. FTP-сервер дозволяє тим, хто складає іспит, переглядати, але не змінювати зміст екзаменаційних файлів. FTP-сервер також приймає і перевіряє студентські імена (логіни) і паролі. Якщо ім'я і пароль збігаються з тими, що зберігаються в базі даних, то студент отримує право на запис і зміну своїх файлів у відповідних директоріях на сервері.

Програмне забезпечення на клієнтських комп'ютерах складається з трьох частин: сервісної, брандмауера і інтерфейсу користувача.

Сервісна частина запускається автоматично і знаходиться в режимі постійного з'єднання з сервером, весь час обмінюючись з ним пакетами. Пакети приймаються через порт 5888. Якщо інформаційне наповнення повідомлення "Start", то в системному реєстрі лічильник набуває значення 120. Це значення буде незмінним впродовж усього процесу отримання пакетів від сервера. Крім цього, сервісна частина перевіряє лічильник на початку іспиту, і, якщо його значення більше "нуля", включається брандмауер. При отриманні пакету з наповненням "Stop" значення лічильника приймає значення "Нуль". У разі виникнення ситуації, коли під час іспиту необхідне перезавантаження комп'ютера, сервісна частина комп'ютера клієнта перевіряє вміст лічильника і, якщо воно більше "нуля", включається брандмауер.

Брандмауер контролює мережний трафік. При включеній системі мережного захисту користувач не може звернутися ні до жодного комп'ютера. Є можливість тільки обміну повідомлення з сервером через порти 5888 – 5892. Кожні 30 секунд через порт 5892 на сервер доставляється пакет з повідомленням про те, що брандмауер включений і іспит продовжується.

Через інтерфейс користувача відбувається завантаження файлів відповідей на сервер.

Програмне забезпечення написане на мові Perl і працює під управління WEB-сервера Apache. На клієнтському боці передбачається використання будь-якого браузера.

Стандартні програми для проведення іспитів, такі, як ExamSoft, Extegrity, SecureExam [2 – 4] використовують комп'ютер як допоміжний засіб. Той, хто складає іспит відповідає на питання тестової програми і відправляє результати на сервер. Програмне забезпечення цих систем блокує комп'ютер під час іспиту і студенти не можуть звернутися до локальної мережі або Інтернету. Після відправлення результатів на сервер, студенти вже не можуть відкорегувати зашифровані відповіді, навіть якщо іспит ще не закінчився і той, хто складає іспит вчасно помітив свою помилку.

При використанні пропонованої автором системи студентові ці можливості доступні. Розроблене програмне забезпечення може використовуватися для будь-яких іспитів, де результатом роботи буде файл з відповідями.

Література: 1. J. P. Barros, L. Estevens, R. Dias, R. Pais, and E.Soeiro, "Using Lab Exams to Ensure Programming Practice in an Introductory Programming Course" // Innovation and Technology in Computer Science Educaton (ITiCSE 03), Thessaloniki, Greece. – June 2003. 2. Securexam web-page, http://www.softwaresecure.com/. 3. Examsoft web-page, http://www.examsoft.com/. 4. Extegrity Exam4 web-page, http://www.extegrity.com/.

УДК 621.396: 621.391 (075.8)

Колесников А. Н.

Колесников С. А.

ИДЕНТИФИКАЦИЯ СИГНАЛОВ ИСТОЧНИКОВ РАДИОИЗЛУЧЕНИЙ НА ОСНОВЕ МЕТОДА ОБУЧЕНИЯ ЛИНЕЙНОГО ПОРОГОВОГО ЭЛЕМЕНТА

Радиочастотный ресурс (РЧР) Украины является стратегическим ресурсом государства. Он обеспечивает предоставление разнообразных телекоммуникационных услуг, являясь составной частью ряда технологий, влияющих как на эффективное функционирование экономики, так и на национальную безопасность государства, определяющих обороноспособность страны, ее информационную безопасность и технологическую независимость.

Государство управляет сферой использования РЧР с помощью системы соответствующих государственных органов на основе законов Украины "Про телекомунікації" [1], "Про радіочастотний ресурс України" [2], постановлениями Кабинета Министров Украины, другими нормативно-правовыми актами.

Среди ряда задач органов управления РЧР одной из основных является обеспечение эффективного использования РЧР, что требует наличия информации о реальном состоянии использования РЧР. Получение такой информации достигается путем организации системы радиочастотного контроля (РЧК).

В настоящее время технической основой системы РЧК в Украине является автоматизированная система РЧК (АСРЧК) [3]. Организационную основу АСРЧК составляют стационарные пос-

ты. Мобильные комплексы (станции) радиомониторинга обеспечивают решение задач РЧК вне зон радиодоступа стационарных постов, а также для уточнения результатов РЧК в пределах городов.

Использование технических средств РЧК на стационарных и мобильных постах позволяет осуществлять контроль использования РЧР и выполнять измерения параметров электромагнитного излучения. В связи с этим определены следующие основные задачи РЧК [4]:

систематический контроль и измерение параметров и характеристик радиоэлектронных средств (РЕС) и источников радиоизлучений;

проведение измерений, связанных с радиопомехами;

идентификация передатчиков и определение класса их излучения путем пеленгации и анализа сигналов;

выявление незаконно действующих передатчиков и подготовка предложений по прекращению их деятельности.

Для решения указанных задач средства РЧК оснащаются соответствующим оборудованием и программным обеспечением. При этом наиболее предпочтительным режимом работы является автоматизированное решение задач РЧК и проведение измерений. Однако в настоящее время многие из операций обработки и анализа принятых сигналов при РЧК выполняются в ручном режиме, что требует существенных временных затрат и наличия высококвалифицированных операторов для обеспечения необходимой точности результата.

В последние годы появилось оборудование РЧК, которое обеспечивает автоматизированную обработку и анализ принятых сигналов на основе хорошо себя зарекомендовавшего корреляционного метода. В частности, данный метод используется для решения задачи идентификации сигналов источников радиоизлучений (ИРИ) [5]. Однако применение корреляционного метода в данном случае имеет ряд ограничений, связанных с видом модуляции сигналов и наполнением электронной базы данных РЕС, которые могут принимать участие в механизме создания радиопомех.

Задача идентификации сигналов ИРИ является одной из наиболее сложных задач РЧК по следующим причинам, во-первых, кратковременного излучения позывных сигналов, во-вторых, использования сокращенных или незарегистрированных позывных сигналов, и в значительной степени − трудности обработки радиосигналов, при передачи которых используются сложные методы кодирования, модуляции и уплотнения информации.

Целью задачи идентификации сигналов ИРИ является установление соответствия того, что в контрольной полосе частот работает именно тот передатчик, который там должен работать, и что параметры его излучения соответствуют тем, что были ему назначены. Результат решения задачи − выявление нелицензионных передатчиков и РЕС, которые нарушают регламент радиосвязи.

Процесс принятия решений об идентификации сигналов ИРИ происходит в условиях неопределенности, быстро меняющейся сигнально-помеховой обстановки, учета большого числа противоречивых требований. В таких условиях хорошо себя зарекомендовали подходы, основанные на идеях и методах теории распознавания и классификации образов [6; 7].

Идентификация сигналов возможна при наличии некоторой исходной информации (или устройств, обеспечивающих ее получение при обучении) о сигналах, требующих классификации. Существующее оборудование РЧМК позволяет принимать сигналы с различными видами модуляции и проводить измерение следующих параметров радиоизлучений [3]:

несущей (или центральной) частоты радиоизлучения;

ширины занимаемой полосы частот радиоизлучения;

уровня принятого сигнала;

параметра модуляции (глубины модуляции для АМ сигналов, девиации частоты для ЧМ сигналов, девиации фазы для ФМ сигналов, разноса частот для частотной телеграфии).

Таким образом, система идентификации сигналов ИРИ может состоять из двух основных частей: входного устройства и устройства принятия решения (классификатора). Во входном устройстве происходит измерение перечисленных параметров радиоизлучений и преобразование их в форму, удобную для дальнейшего анализа. Результаты этого преобразования дают n -мерный вектор:

$$X = (x_1, x_{2,\ldots,} x_n), \tag{1}$$

который будем называть кодом объекта, где $x_1, x_{2,\ldots,} x_n$ − числовые значения признаков (параметров) радиоизлучений. Тогда совокупность векторов, соответствующих объектам R различных классов (образов), образуют отдельные области $R_i (i = \overline{1,R})$ в n-мерном пространстве кодов объектов.

Задача идентификации сигналов ИРИ состоит в построении в пространстве X^n поверхности, разделяющей множество областей R_i, отвечающих различным классам излучений. Это построение выполняется по появляющимся в процессе “обучения” векторам X , о каждом их которых “учитель” дополнительно сообщает классификатору о принадлежности его к конкретному классу. После построения такой поверхности новые векторы будут идентифицироваться классификатором в зависимости от их положений относительно разделяющей поверхности.

Разделяющие поверхности любого классификатора объектов можно полностью определить R скалярными функциями $g_1(X)$, ... , $g_R(X)$, которые называются дискриминантными функциями (ДФ) [6]. ДФ выбираются так, чтобы выполнялось условие:

$$\forall X \in R_i \quad g_i(X) > g_j(X) \text{ при } i, j = 1,2,\ldots R, \; i \neq j, \tag{2}$$

то есть *i*-я дискриминантная функция на области R_i принимает наибольшее значение по сравнению с другими ДФ. Тогда поверхность, разделяющая смежные области R_i и R_j, определяется уравнением

$$g_i(X) - g_j(X) = 0. \quad (3)$$

Простоты ради будем рассматривать линейные ДФ вида

$$g(X) = \sum_{i=1}^{n} \omega_i x_i + \omega_{n+1} = X \cdot W + \omega_{n+1}, \quad (4)$$

где $\omega_i (i = 1, \ldots, n)$ – весовые коэффициенты, или компоненты вектора весов $W = (w_1, w_2, \ldots, w_n)$.

Пусть $\mathbb{X} = \{X_1, \ldots, X_M\}$ – конечное множество объектов $X_j (j = \overline{1, M})$, которые классифицированы так, что каждый объект принадлежит только одному из *R* классов (образов). Такая классификация разбивает $\mathbb{X}$ на множество $\mathbb{X}_1$,..., $\mathbb{X}_R$ так, что каждый объект принадлежит классу $i\ (i = \overline{1, R})$. Назовем $\mathbb{X}_i$ обучающими выборками. Если существует линейное правило классификации (ПК), правильно относящее каждый объект $X_i \in \mathbb{X}_n$ к соответствующему классу, то подмножества $\mathbb{X}_1$,..., $\mathbb{X}_R$ называются линейно разделимыми и имеем дело с линейной классификацией.

Другими словами, если распознаваемые образы R_1 , ... , R_R в X^n линейно разделимы, то существуют такие линейные ДФ $g_1(X)$, ... ,$g_R(X)$, что

$$\begin{array}{ll} g_i(X) > g_j(X) & \forall X \in \mathbb{X}_i, \\ j = 1, \ldots, R; \ j \neq i & \forall i = 1, \ldots, R \end{array} \quad (5)$$

и можно машинным путем извлечь новые знания в форме распознающего правила (закономерности) $\Phi(X)$:

$$\Phi(X) = g_i(X) = \max\{g_1(X), g_2(X), \ldots, g_R(X)\}, \text{ если } X \in \mathbb{X}_i. \quad (6)$$

В случае двух классов ($R = 2$) искомые знания описываются в форме ПК:

$$\begin{cases} g(X) > 0, \text{ если } X \in \mathbb{X}_1, \\ g(X) < 0, \text{ если } X \in \mathbb{X}_2. \end{cases} \quad (7)$$

Обучение будем выполнять с помощью алгоритма извлечения классифицирующих знаний методом обучения линейного порогового элемента (ЛПЭ), реализующего подбор весов $w_1, \ldots, w_n$.

Линейным пороговым элементом называется устройство, реализующее линейную ДФ вида (4) так, что на выходе ЛПЭ появляется сигнал "+1", если $g(X) > 0$, и "−1" – если $g(X) < 0$. Блок-схема ЛПЭ показана на рисунке.

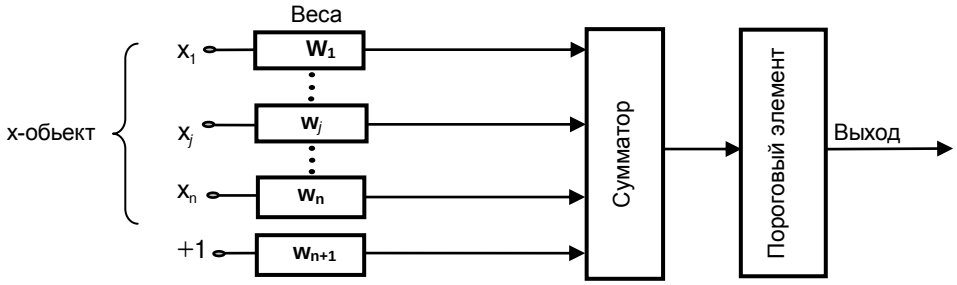


Рис. **Блок-схема ЛПЭ**

Задача состоит в том, чтобы "научить" ЛПЭ с помощью искомого алгоритма формировать на выходе "+1" при появлении на его входе объекта $X \in K_1$ и сигнал "−1" при появлении любого объекта $X \in K_2$.

Рассмотрим алгоритм, предусматривающий итерационный процесс корректировки весов w_i, соответствующий последовательному изменению положения и ориентации гиперплоскости, разделяющей классы K_1 и K_2.

Для уяснения этого процесса введем расширенный вектор – объект Y:

$$Y = (y_1, y_2, \ldots, y_D), \quad (8)$$

где $y_i = x_i$, $D = n + 1$, $y_D = +1$, $i = 1,2,\ldots,n$, и перейдем в новое пространство весов $W^D = \{w_1, \ldots, w_n, w_{n+1=D}\}$.

В пространстве W^D линейная ДФ вида

$$g(X) = Y \cdot W = 0 \tag{9}$$

определяет гиперплоскость и называется плоскостью объекта (ПО). ПО делит пространство W^D на два класса так, что те из точек W, которые для объекта Y обеспечивают на выходе "+1", лежат по одну сторону гиперплоскости (положительная сторона), а по отрицательную сторону располагаются точки, дающие на выходе ЛПЭ "–1".

Предположение о линейной разделимости K_1 и K_2 означает, что существует вектор W, называемый решающим весовым вектором, такой, что

$$\begin{cases} Y \cdot W > 0, & \text{для } \forall\, Y \in K_1, \\ Y \cdot W < 0, & \text{для } \forall\, Y \in K_2. \end{cases} \tag{10}$$

Вектор W можно определить по обучающей выборке с помощью алгоритмов с исправлением ошибок в процессе циклического предъявления обучающих объектов Y.

Если, например, для некоторого объекта $Y \in K_1$ с весом W на выходе ЛПЭ имеем "−1" (то есть $Y \cdot W < 0$) вместо $Y \cdot W > 0$, что означает ошибку, или $Y \cdot W = 0$, то есть выход не определен, то эту ошибку можно исправить, перенося W в точку на положительной стороне плоскости объекта. Это можно осуществить кратчайшим путем по линии, перпендикулярной к ПО (9), то есть добавляя к W вектор объекта Y и получая таким образом новый весовой вектор W', равный

$$W' = W + CY, \tag{11}$$

где C − положительное число, называемое коэффициентом коррекции.

Для достаточно больших C точка весов W' перейдет на другую сторону гиперплоскости и $Y \cdot W' > 0$. Если бы W по ошибке попал бы на положительную сторону плоскости объекта, то тогда

$$W' = W - CY. \tag{12}$$

Итак, обобщая выражения (11), (12), при $C = 1$ алгоритм обучения примет вид:

$$W_{n+1} = \begin{cases} W_n + Y_i, & \text{если } Y_i \in K_1 \text{ и } Y \cdot W < 0; \\ W_n - Y_i, & \text{если } Y_i \in K_2 \text{ и } Y \cdot W > 0. \end{cases} \tag{13}$$

Начальный вектор W в алгоритме (13) выбирается случайно либо равным 0.

Проиллюстрируем применение описанного метода для идентификации сигналов базовых станций цифровой сотовой радиосвязи стандарта CDMA-800 (класс радиоизлучения 1M25G1D) и GSM-900 (класс радиоизлучения 271KG7W), которые работают на радиочастотах передачи f_{CDMA} и f_{GSM} соответственно.

В качестве элементов x_i вектора признаков объекта $X_j = (x_1, x_2, \ldots, x_5)$ будем использовать измеренные основные параметры радиоизлучений: значения частот передачи $x_1 - f_{CDMA}$, $x_2 - f_{GSM}$; полос частот на контрольном уровне $x_3 - B_{к.CDMA}$, $x_4 - B_{к.GSM}$; признак модуляции $x_5 - M_ф$ (фазовая модуляция для рассматриваемых радиоизлучений). При этом авторы считают, что признак принимает значение "1", если соответствующий параметр находится в пределах установленной нормы, и "0", если параметр выходит за установленные пределы.

Сформируем обучающую выборку возможных ситуаций:

$X_1 = (1, 0, 1, 0, 1)$ − радиоизлучение станции стандарта CDMA;
$X_2 = (0, 1, 0, 1, 1)$ − радиоизлучение станции стандарта GSM;
$X_3 = (1, 0, 0, 1, 1)$ − радиоизлучение станции стандарта CDMA;
$X_4 = (0, 1, 1, 0, 1)$ − радиоизлучение станции стандарта GSM;
$X_5 = (1, 0, 0, 0, 1)$ − радиоизлучение станции стандарта CDMA;
$X_6 = (0, 1, 0, 0, 1)$ − радиоизлучение станции стандарта GSM;
$X_7 = (0, 0, 1, 0, 1)$ − радиоизлучение станции стандарта CDMA;
$X_8 = (0, 0, 0, 1, 1)$ − радиоизлучение станции стандарта GSM.

Целью обучения ЛПЭ с использованием алгоритма (13) является нахождение такой линейной ДФ $g(X)$, разделяющей пространство объектов на два класса $X_1 = \{X_1, X_3, X_5, X_7\} \in K_1$ (радиоизлучение станции стандарта CDMA) и $\boldsymbol{x}_2 = \{X_2, X_4, X_6, X_8\} \in K_2$ (радиоизлучение станции стандарта GSM), что:

$$g(X) = \begin{cases} +1, & \text{если } X \in K_1 \text{ (радиоизлучение станции стандарта CDMA),} \\ -1, & \text{если } X \in K_2 \text{ (радиоизлучение станции стандарта GSM).} \end{cases}$$

Для достижения поставленной цели составим обучающую выборку расширенных векторов объектов Y согласно (8) с указанием их принадлежности к образцу и поместим их в таблицу.

Таблица

Обобщенная таблица векторов

№ п/п	y_1	y_2	y_3	y_4	y_5	y_6	Выход ЛПЭ
1	1	0	1	0	1	1	+1
2	0	1	0	1	1	1	- 1
3	1	0	0	1	1	1	+1
4	0	1	1	0	1	1	- 1
5	1	0	0	0	1	1	+1
6	0	1	0	0	1	1	- 1
7	0	0	1	0	1	1	+1
8	0	0	0	1	1	1	- 1

Принимая за начальный весовой вектор $W_0 = (0, 0, 0, 0, 0, 0)$ и C = 1, осуществляем итерации согласно алгоритма (13). Обучение заканчивается (то есть алгоритм сходится) на 4-й итерации после 25-и предъявленных объектов и с 12-ю исправлениями весов. В результате получены знания в форме следующей линейной классифицирующей ДФ:

$$g(Y) = 3y_1 - 3y_2 + 2y_3 - 2y_4 + 1 \cdot$$

На примере метода обучения линейного порогового элемента показана применимость технологии распознавания образов для задачи идентификации сигналов ИРИ. Исходя из этого, одним из перспективных направлений работы в этой области является использование искусственных нейронных сетей, что позволит реализовать параллельно распределенный процессор, обеспечивающий достоверную автоматическую идентификацию сигналов ИРИ.

Литература: 1. Збірник нормативно-правових актів у сфері телекомунікацій та користування радіочастотним ресурсом / Уклад. В.І. Кіріченко, Н.А. Письменчук, М.В. Гріцаєнко та ін.; За ред. П.В. Слободянюка. – Ніжин: ТОВ "Видавництво "Аспект-Поліграф", 2006. – 800 с. 2. Ступак В. С. Основи радіочастотного контролю: Практичний посібник / В. С. Ступак, С. О. Долматов / За ред. В. Ф. Олійника. – К.: УДЦР, 2004. – 219 с. 3. Справочник по радиоконтролю. – Женева: МСЭ, 1995. – 442 с. 4. Ральников В. И. Идентификация источников помех с помощью корреляционного регистратора / В. И. Ральников, И. П. Харченко // Электросвязь. – 2001. – № 9. – С. 23 – 29. 5. Ту Дж. Принципы распознавания образов / Ту Дж., Р. Гонсалес. – М.: Мир, 1978. – 412 с. 6. Сироджа И. Б. Структурно-аналитические модели и алгоритмы распознавания и идентификации объектов управления / И. Б. Сироджа, В. Г. Тупало, С. В. Левин. – К.: Техніка, 1993. – 204 с.

УДК 65.012.8

Кавун С. В.

ЖИЗНЕННЫЙ ЦИКЛ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Экономическими и информационными аспектами разработки, внедрения и использования занимались многие отечественные и зарубежные специалисты и ученые [1 − 5], но еще существует достаточно нерешенных вопросов теоретического и практического характера.

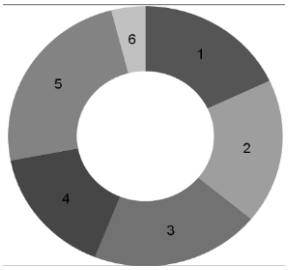
Одним из таких нерешенных в достаточной степени вопросов является исследование жизненного цикла системы экономической безопасности (СЭБ) предприятия. Актуальность исследования подтверждается следующими фактами. За последние годы по данным исследования CSI Computer Crime and Security Survey ущерб, наносимый предприятиям в результате компьютерных махинаций, возрос в несколько раз и составил несколько миллиардов долларов в год. По всем составляющим видам сетевых атак на предприятия виден очевидный рост активности. Лишь 20% предприятий готовы или начали развивать СЭБ. Однако мало кто представляет, с чего начинается создание грамотно построенной СЭБ предприятия, каков жизненный цикл его развития, как контролировать и улучшать.

На эти и ряд других вопросов признана ответить предлагаемая статья. Также целью статьи является наглядный показ механизма развития СЭБ на всем временном интервале.

Как показали проведенные исследования (на основе социологического опроса специалистов различных предприятий в анкетной форме), распределение весовых коэффициентов влияния различных факторов на общий уровень функционирования СЭБ предприятия выглядит в форме, представленной на рис. 1.

Если рассматривать в качестве критерия функционирования СЭБ предприятия уровень ЭБ, достигаемый при ее использовании, то необходимым и достаточным условием его актуальности будет динамизм отслеживания и своевременная реакция на изменение. Тем самым будет достигаться всесторонний контроль СЭБ в реальном масштабе времени.

Применим понятия теории систем к описанию СЭБ предприятия.



1 – коэффициент влияния нормативных актов, k_1 = 18%;
2 – коэффициент влияния настроек ОС, k_2 = 18%;
3 – коэффициент влияния настроек СЭБ предприятия, k_3 = 20%;
4 – коэффициент влияния правил эксплуатации, k_4 = 16 %;
5 – коэффициент влияния степени отказоустойчивости СЭБ, k_5 = 24%;
6 – коэффициент влияния других факторов, k_6 = 4%.

Рис. 1. **Распределение весовых коэффициентов**

Следовательно, суммарный вес влияния факторов будет равен

$$K = \frac{1}{100} \sum_{i=1}^{n} k_i,$$

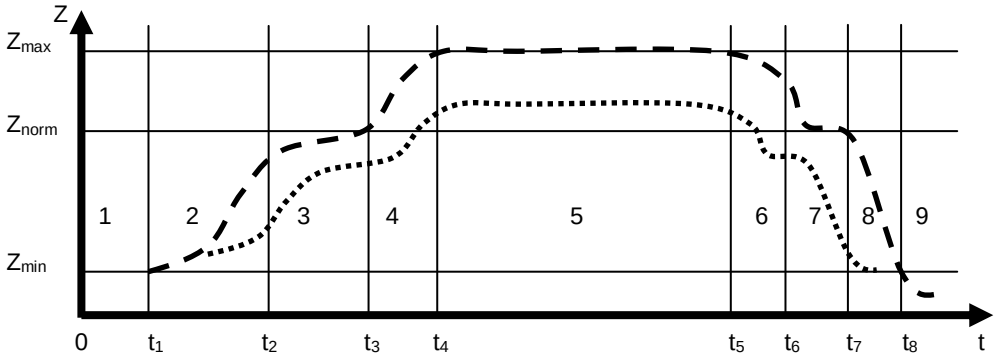
где n = 6.

С течением времени уровень ЭБ на предприятии, обеспечиваемый разработанной и внедренной СЭБ, растет. Это связано с рядом факторов, среди которых можно выделить следующие:

1) дополнительные инвестиции;
2) повышение уровня подготовки самих специалистов по ЭБ;
3) выявление и устранение недостатков;
4) выявление и устранение уязвимостей, брешей, люков.

Далее, как и для всех подобных систем, уровень ЭБ может достигнуть (а может и не достигнуть) своего максимального значения. Это может означать для предприятия появление экономического эффекта от внедрения, выявление всех недостатков и уязвимостей, выход СЭБ на потенциально максимальную мощность работы.

Время жизненного цикла СЭБ (рис. 2) на предприятии в фазе 1 никогда не равно 0, поскольку такие системы на предприятиях не создают с самого начала, а внедряют некие прототипы, которые потом в процессе начальной эксплуатации "затачивают" под потребности самого предприятия. Кстати говоря, по аналогичной схеме используется программное обеспечение фирмы 1С.



Условные обозначения:
Фазы жизненного цикла:
1: [0; t_1) – фаза возникновения необходимости разработки СЭБ;
2: [t_1; t_2) – фаза начала эксплуатации СЭБ на предприятии СЭБ;
3: [t_2; t_3) – фаза выхода на заданный нормальный уровень функционирования СЭБ на предприятии;
4: [t_3; t_4) – фаза усовершенствования и модификации СЭБ;
5: [t_4; t_5) – фаза обеспечения окупаемости, возврата инвестиций, отдачи при использовании;
6: [t_5; t_6) – фаза первичных признаков износа, устаревания, функциональных сбоев;
7: [t_6; t_7) – фаза принятия превентивных мер, обновления, модернизации, реструктуризации;
8: [t_7; t_8) – фаза окончательного снижения функциональности, морального устаревания, выхода из строя, возникновения отказов;
9: [t_8; ∞) – фаза вывода из эксплуатации СЭБ на предприятии.
Уровни ЭБ на предприятии:
Z_{min} – минимальный уровень ЭБ, достигаемый в начальной и конечной стадиях эксплуатации СЭБ;
Z_{norm} – нормальный уровень ЭБ, при котором предприятие выполняет основные свои функции;
Z_{max} – максимальный уровень ЭБ, достижение которого обеспечивает экономический рост, при этом часто $Z_{max} = Z_{norm}$.

Рис. 2. **Фазы жизненного цикла СЭБ предприятия**

Конечное время жизненного цикла СЭБ на предприятии всегда существует и на сегодня оно соответствует времени существования (актуальности) любой ИТ-технологии. По оценкам экспертов это время в пределе равно от 0,5 до 1,5 лет. По истечении данного промежутка времени происходит моральное устаревание используемых технологий, а следовательно, и построенного на их основе программного обеспечения, и как следствие – используемой СЭБ предприятия.

Производя регулярный мониторинг СЭБ предприятия, следует помнить о практически возможном (показан точечной линией на рис. 2) и теоретически достигаемом уровне ЭБ. Между тем всегда в любых системах существовала разница, обеспечиваемая различными стохастическими событиями, непредвиденными действиями персонала предприятия, форс-мажорными обстоятельствами и другими природными факторами. Естественно, в пределах каких-то фаз эти уровни могут совпадать, но, в основном, это начальная и конечная фазы (фазы 1 и 9 на рис. 2).

На какой-то произвольной фазе совокупностью воздействия на СЭБ предприятия суммарной доли коэффициентов k2 – k6 может оказать существенное влияние, уровень ЭБ предприятия оказывается вне сферы влияния нормативных актов. То есть суммарный воздействующий потенциал составляет 78%. Это может привести к резкому снижению текущего уровня ЭБ на предприятии, как показано сплошной линией на рис. 3.

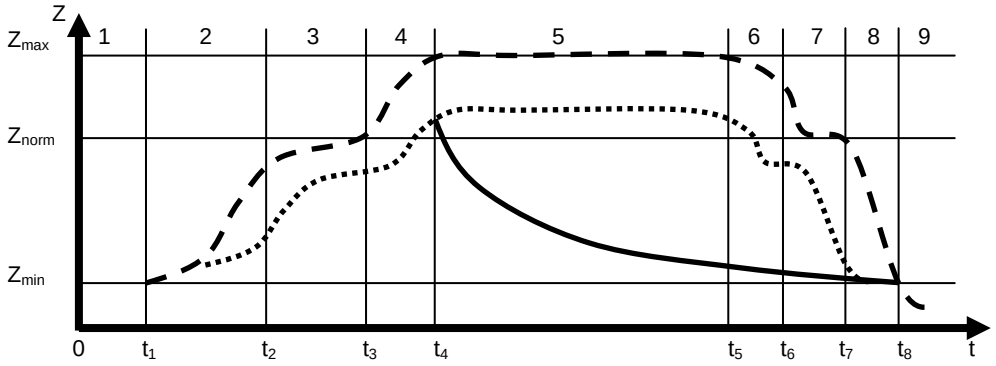


Рис. 3. **Этап воздействия коэффициентов $k_2 - k_6$ на СЭБ**

Все это приводит к необходимости проведения внеочередного мониторинга (аудита) СЭБ предприятия с целью выявления, устранения и дальнейшего предотвращения подобных провалов, так как их совокупность может вообще поставить вопрос о целесообразности использования СЭБ на предприятии.

На предприятиях с длительным жизненным циклом использования СЭБ (не один-два года, а десяток и более лет), как правило, к периодическим аудитам привыкают. Но иногда может потребоваться отдельный внеплановый аудит. Необходимость во внеплановом аудите может появиться, если в какой-то области происходит технологический прорыв, например, руками хакеров создан новый хитрый "червь" или разработан эффективный метод взлома алгоритмов шифрования. Подобные ситуации становятся сигналом к тому, чтобы пересмотреть весь механизм функционирования СЭБ.

Еще один вариант развития деятельности предприятия необходимо рассмотреть – это возникновение новой формы или слияние, модификация структуры, стратегическое партнерство с другими (может быть и венчурными) компаниями.

В этом случае необходимость проведения внепланового аудита СЭБ предприятия возникает естественным путем. Кроме того, в ходе проводимой реорганизации такая необходимость может возникать несколько раз, например, аудит проводится с одной стороны (фирмой-партнером), а потом другим партнером. По итогам двух независимых мероприятий проводится сравнительный анализ. Тогда уровень ЭБ на предприятии может снижаться на данном промежутке времени несколько раз, как это показано сплошной линией на рис. 4.

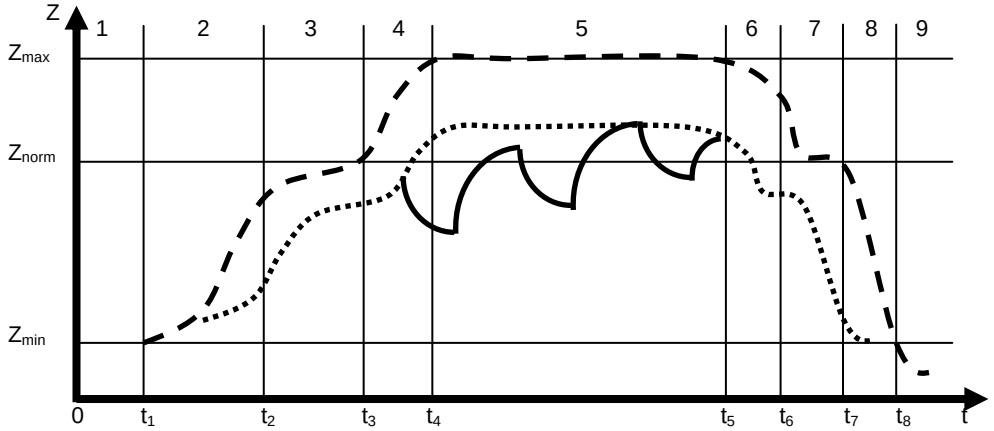


Рис. 4. **Этапы проведения серии аудиторских проверок**

Кроме того, если предприятие имеет несколько удаленных подразделений (офисов, филиалов), то может возникнуть ситуация, когда локальное изменение уровня ЭБ не отображается на ходе развития общего уровня при использовании СЭБ предприятия. Тогда необходимость проведения внеплановых аудитов удаленных подразделений возникает чаще и требует введения централизованной системы аудита всех дочерних структур предприятия.

Таким образом, при использовании серии плановых и внеплановых аудиторских проверок можно выдерживать оптимальный итоговый (общий, суммарный) уровень ЭБ предприятия, который будет в среднем соответствовать нормальному или заданному необходимому уровню ЭБ.

В соответствии с этими мероприятиями жизненный цикл СЭБ предприятия приобретает более равномерный характер, что может свидетельствовать о правильном внедрении и реализации СЭБ на предприятии.

Практика исследований на предприятиях Харькова и области показывает, что за два года уровень ЭБ предприятия может снизиться на 10 – 30%. Можно предположить, что если снижение ЭБ с оптимального уровня до нуля нанесет убыток в 100% (например, 10 млн. грн.), то уменьшение на 30% чревато убытком в 3 млн. грн., например при проведении аудиторской проверки удаленных подразделений предприятия. Соответственно, возможные потери на предприятии нужно оценивать исходя из того, что за пару лет произойдет снижение уровня безопасности всех доходных бизнес-процессов на 30%. Однако следует не забывать, что это теоретическая апостериорная оценка, которая в отдельных случаях может отличаться от реальной практической оценки.

В результате может возникнуть мнение, что проведение аудиторных проверок приводит к непредвиденным финансовым затратам и для самого предприятия – экономически не выгодно. Это не так, поскольку речь идет только о первичных затратах и не оговариваются последующие доходы предприятия в виде экономии финансовых средств, полученные в результате предотвращения различных экономических, финансовых, информационных и других видов потерь. Некоторые виды потерь можно рассчитать в денежном эквиваленте с помощью различных методик, например предложенной автором в работе [6].

"Время от времени необходимо проводить комплексную проверку СЭБ, чтобы выявлять бреши и устранять их до того, как этим воспользуются злоумышленники либо сойдутся вместе неблагоприятные факторы" – таков общий вывод всех профессиональных ИТ-специалистов [7].

Иногда аудиторские проверки проводят фирмы, специализирующиеся в этой области. Тогда, как правило, они выполняют весь комплекс работ таким образом, чтобы предлагаемое решение (например, разработка СЭБ предприятия) было подготовлено под их же собственное предложение. С одной стороны, это может быть положительным фактором, например для снижения стоимости выполняемых работ и оказываемых услуг. Однако, с другой стороны, руководителей предприятия это может лишить возможности проведения независимого анализа предлагаемых на рынке средств и существенно ограничит правильность выбора оптимального решения.

Как правило, взаимодействие с фирмой-аудитором состоит из нескольких этапов. На первом этапе выполняется работа аудитора и формируется отчет о том, какие бизнес-процессы выполняются на предприятии, каковы их взаимосвязи. Грамотный аудитор составит отчет так, что будет видно, где и какого рода уязвимости [7] имеются в системе, к каким последствиям они могут привести и каковы возможные потери [6].

К сожалению, не всегда специалист-аудитор дает четкие и конкретные рекомендации, каким образом эти уязвимости устраняются, поэтому необходимо требовать от него, чтобы в отчете содержался раздел, который можно назвать техническим заданием на модернизацию СЭБ предприятия. Другими словами, отчет должен содержать внятные рекомендации, но не советы, что и где нужно покупать. При этом необходимо помнить, что подобный отчет является юридическим документом, завизированным аудитором.

Следующий этап – составление подробного технического задания, с которым можно обратиться в любую профильную компанию, занимающуюся экономической или информационной безопасностью. Если проведением аудита предприятия, затем разработкой проекта модернизации СЭБ, поставками техники и ПО занималась одна компания, то все этапы будут логично связаны между собой и разногласия на их стыках сведутся к минимуму.

Если же перед специалистом (сотрудником предприятия или фирмы-аудитором) по ЭБ стоит задача решить реальную проблему в рамках предполагаемого (выделяемого) бюджета, то придется идти по иному пути, для каждого из этапов выбирая в ходе тендера исполнителя, способного лучше других (дешевле) решить поставленные задачи. В этом случае у предприятия появляется широкий спектр возможностей для оптимизации расходов. Здесь также следует помнить, что "скупой платит дважды", то есть снижение расходов на СЭБ предприятия может негативно отразиться на итоговом уровне ЭБ и привести к значительным финансовым потерям. Этот эффект известен как "эффект бумеранга".

Кроме того, не следует забывать о человеческом факторе, на котором базируется уровень подготовки персонала. На сегодня у многих аудиторов есть в использовании множество различных тестов, позволяющих выявлять до 80–90% случаев непрофессиональных действий сотрудников предприятий.

В качестве дальнейшего развития данного вопроса можно предложить проведение исследований жизненного цикла СЭБ предприятия при его влиянии на основные экономические показатели развития предприятия, среди которых можно выделить чистый оборотный капитал (NWC), коэффициент текущей ликвидности (CR), коэффициент рентабельности активов (ROA) и др.

Литература: 1. Олейников Е. А. Экономическая и национальная безопасность: Учебник для вузов. – М.: Экзамен, 2005. – 768 с. 2. Ярочкин В. И. Система безопасности фирмы. – М., 1997. – 185 с. 3. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС", 2001. – 688 с. 4. Дорошев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно "Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)", США, "Оранжевая книга" / В. В. Дорошев, В. В. Домарев // Бизнес и безопасность. – 1998. – №1. – С. 19 – 21. 5. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. – Х., 2006. – 240 с. 6. Кавун С. В. Оцінка збитку організації внаслідок мережних атак на її ресурси // Економіка розвитку. – 2007. – №1(41).– С. 83 – 85. 7. Кавун С. В. Информационная безопасность в бизнесе. – Харьков: Изд. ХНЭУ, 2007. – 408 с.

УДК 004.056.5:518

Кобозева А. А.

ТЕОРИЯ ВОЗМУЩЕНИЙ КАК ОСНОВНОЙ ИНСТРУМЕНТ АНАЛИЗА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И СВОЙСТВ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

Современное общество вступает в информационный период своего развития [1]. В связи с этим проблема информационной безопасности, решение которой неотделимо от анализа состояния информационных объектов (ИО), является чрезвычайно значимой и актуальной [1; 2]. До настоящего времени оставался нерешенным вопрос создания единого математического подхода к такому анализу. Используемый здесь математический аппарат является недостаточным для всестороннего описания объектов, которые плохо формализуются, обладают свойствами, плохо известными априори и изменяющимися в процессе функционирования, каковой является любая информационно-технологическая система (ИТС).

Цель работы − создание основ единого математического подхода к оценке состояния существующих и генерируемых ИО, в том числе систем защиты информации в целом, основанного на теории возмущений [3; 4]. Такой подход даст принципиальную возможность для определения степени зависимости состояния ИО от возмущающего воздействия, позволит производить оценку свойств объекта, анализировать результат воздействия, абстрагируясь от их конкретики.

Для достижения поставленной цели необходимо решить следующие задачи: разработать общие формальные модели произвольных непрерывного и дискретного информационных процессов (ИП); на основании разработанных моделей выделить набор параметров, анализ возмущений которых определяет характеристики исследуемых процессов (объектов).

При формальном представлении любого, в том числе и информационного, процесса в виде его математической модели выделяется конечное множество основных параметров (входных и выходных), несущих в себе всю ценную информацию об основных закономерностях процесса [3], который характеризуется приведением выходных параметров в соответствие с входными по некоторому закону. Любой ИП в самом общем виде можно формально представить как некоторую непрерывную вектор-функцию [5] конечного числа переменных:

$$\Phi(x_1,...,x_n)=\begin{pmatrix}\varphi_1(x_1,...,x_n)\\ \varphi_2(x_1,...,x_n)\\ \vdots\\ \varphi_m(x_1,...,x_n)\end{pmatrix}=\begin{pmatrix}\Phi_1\\ \Phi_2\\ \vdots\\ \Phi_m\end{pmatrix}, \quad (1)$$

где $(\Phi_1,\Phi_2,...,\Phi_m)\in R^m$ – выходные параметры;

$(x_1,...,x_n)\in D(\Phi)\subseteq R^n$ – входные параметры.

Функция (1), порождает m вещественных функций

$$\varphi_i(x_1,...,x_n)=\Phi_i,\ \ i=\overline{1,m} \tag{2}$$

на области определения $D(\Phi)$ [5].

Утверждение 1. Произвольный непрерывный ИП (или ИО, рассматриваемый как результат процесса его синтеза) может быть формально представлен в виде конечного множества вещественных функций (2), а анализ этого процесса сведен к анализу полученных функций.

Построение функции (1) для реального ИП (ИО) предполагает дискретность входных параметров, являющихся результатами измерений, экспериментов и т. д. Кроме того, процесс обработки (1) с использованием вычислительных средств и численных методов так или иначе приведет к ее предварительной дискретизации (и квантованию), результатом которой будет n-мерная матрица с элементами из R^m. С учетом того, что функция (1) порождает m функций (2), результат дискретизации может быть представлен как множество, состоящее из m n-мерных матриц $M_1, M_2,..., M_m$ с элементами из R, каждая из которых соответствует функции (2).

Утверждение 2. Произвольный ИП (или ИО, рассматриваемый как результат процесса его синтеза) может быть формально представлен в виде конечного множества матриц конечной размерности с вещественными элементами, а анализ процесса принципиально можно свести к матричному анализу.

Как показывает практика, с учетом удобства обработки получаемой модели чаще всего при моделировании реальных ИП и ИО используются двумерные матрицы, которые и будут рассматриваться ниже.

Замечание. Если в полученной при моделировании ИП (ИО) совокупности $M_1, M_2,..., M_m$ матриц $n>2$, то любой M_j, $j=\overline{1,m}$, можно поставить в соответствие конечное множество матриц размерности 2, каждая из которых получается из M_j путем фиксирования в ней всех индексов, кроме двух.

Пусть математической моделью некоторого ИО является $k\times k$ матрица F ($n=2$). Результат любых действий, производимых над объектом в общем случае можно представить как возмущение ΔF матрицы F, а задача любого преобразования объекта, то есть генерации нового объекта, – это задача получения возмущенной матрицы $\overline{F}$ для F, причем

$$\overline{F}=F+\Delta F, \tag{3}$$

где $\Delta F=f(F)$, то есть ΔF является некоторой функцией матрицы F.

Из соотношения (3) вытекает истинность следующего утверждения.

Утверждение 3. Преобразования ИО эквивалентным образом представимы в виде элементарных матричных операций.

В качестве набора параметров, однозначно определяющих и всесторонне характеризующих любой ИО, можно использовать множество сингулярных чисел (СНЧ) и ортонормированных лексикографически положительных сингулярных векторов (СНВ) соответствующей ему матрицы или, в случае ее симметричности, спектр и множество лексикографически положительных ортонормированных собственных векторов (СВ), которые являются результатом нормального сингулярного (SVD) или нормального спектрального разложения (СР) матрицы соответственно, однозначно определяют матрицу [6], а значит и отвечающий ей ИО. Назовем такие наборы параметров полными.

Любое преобразование объекта возмутит его матрицу F, а значит множество СНЧ и СНВ (СЗ и СВ).

Утверждение 4. Преобразование ИО эквивалентным образом представим в виде совокупности возмущений СНЧ и (или) СНВ (СЗ и (или) СВ) его матрицы, определяемых нормальным SVD (СР), что позволяет свести задачу анализа процесса преобразования и состояния объекта к анализу возмущений СНЧ и СНВ (СЗ и СВ), а задачу синтеза объекта с заданными свойствами – к задаче обеспечения определенных характеристик возмущений СНЧ и СНВ (СЗ и СВ) его матрицы.

Для СНЧ $\sigma_j(F)$, $\sigma_j(F+\Delta F)$, $j=\overline{1,k}$ матриц F и $F+\Delta F$ соответственно имеет место соотношение [4]:

$$\max_{1\le j\le N}\left|\sigma_j(F)-\sigma_j(F+\Delta F)\right|\le\left\|\Delta F\right\|_2, \tag{4}$$

где $\left\|\bullet\right\|_2$ – спектральная матричная норма [4].

Аналогичное соотношение имеет место и для СЗ $\lambda_j(F)$ симметричной матрицы F [7]. В силу соотношения (4) СНЧ (СЗ) матрицы являются нечувствительными к возмущающим воздействиям независимо от того, чувствительной или нечувствительной окажется задача по формированию $F+\Delta F$. Таким образом, для оценки чувствительности задачи преобразования ИО с матрицей F имеет смысл анализировать лишь возмущения СНВ (СВ) F, которые произошли в ходе преобразования, рассматривая результат преобразования объекта в виде совокупности возмущений СНВ (СВ) его матрицы.

Утверждение 5. Чувствительность задачи, состоящей в произвольном преобразовании ИО, будет определяться чувствительностью возмущенных преобразованием объекта СНВ (СВ) его матрицы [6; 8].

Пусть построенная матричная модель ИП (ИО) используется для анализа возмущающего воздействия. Такой анализ сведется к анализу возмущений СНЧ (СЗ) соответствующей матрицы, поскольку, в соответствии с (4), возмущения СНЧ (СЗ) сравнимы с величиной возмущающего воздействия, чего нельзя в общем случае сказать о СНВ (СВ) [6; 8].

Создание научного базиса для обработки данных об ИО невозможно без наличия адекватной математической модели СЗИ. В работе [9] предлагается принципиально новая универсальная графово-матричная математическая модель ИТС, основанная на принципах функционирования нервной системы человека, разработанная на базе теории возмущений. Получение и использование такой модели находится в полном соответствии с утверждениями 2, 3, анализ состояния ИТС сводится к анализу соответствующей (симметричной) матрицы, состоящему в исследовании совокупности возмущений ее СЗ и (или) СВ (утверждение 4).

В настоящей работе на базе теории возмущений заложены основы единого подхода к оценке состояния произвольных существующих и создаваемых ИО, в том числе систем защиты информации в целом, без чего немыслимо создание интенсивной системы комплексного обеспечения безопасности информационных технологий. Показано, что решение задач, связанных с оценками свойств ИО и процессов их функционирования, независимо от задачи и конкретики объекта, сводится к анализу возмущений полных наборов параметров соответствующих матриц, которые произошли в ходе формирования объекта (при прохождении процесса), или подмножеств полных наборов. Отсутствие в открытой печати аналогичных подходов в нашей стране и за рубежом делает результаты исследований приоритетными.

Литература: 1. Куприянов А. И. Основы защиты информации / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М.: Изд. центр "Академия", 2006. – 256 с. 2. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 502 с. 3. Маслов В. П. Асимптотические методы и теория возмущений. – М.: Наука, Гл. ред. физ.-мат. лит., 1988. – 312 с. 4. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. – 430 с. 5. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления. Том I. – М.: Наука, 1969. – 608 с. 6. Кобозева А. А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах // Вісн. Східноукр. нац. ун-ту ім. В. Даля. – 2006. – №9(103). – Ч. 1. – С. 74 – 82. 7. Парлетт Б. Симметричная проблема собственных значений. Численные методы: Пер. с англ. – М.: Мир, 1983. – 384 с. 8. Кобозева А. А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // Искусственный интеллект. – 2007. – №4. – С. 531 – 538. 9. Кобозева А. А. Модель системы защиты информации, основанная на принципах естественной системы управления / А. А. Кобозева, В. А. Хорошко // Захист інформації. – 2007. – Спецвипуск. – С. 56 – 62.

УДК 65.012.8

Безмалый В. Ф.

ОРГАНИЗАЦИЯ ПОСТРОЕНИЯ ОТДЕЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сегодня сложно найти организацию, в которой никто и никогда не задумывался бы о защите информации. Со всех сторон доносится информация о взломах, вирусах, вредоносном программном обеспечении (ПО), атаках, угрозах, уязвимостях.

Информационная безопасность (ИБ) должна восприниматься как комплекс организационно-технических мер, поскольку, как отмечалось ранее, обеспечить конфиденциальность, целостность

и доступность нельзя ни отдельно взятыми техническими мерами, ни организационными мерами. Можно привести этому массу примеров [1; 2].

В практике работы существует ряд нерешенных проблем. Например, если принято решение обеспечивать защиту только техническими мерами, но при этом организационные документы отсутствуют (так часто бывает, если защитой занимается отдел ИТ или начальник отдела ИБ бывший представитель ИТ-структур. Что в этом случае произойдет? Предположим, что сотрудник организации систематически передает конфиденциальную информацию по электронной почте конкурентам и была обнаружена утечка. Если нет документов, следовательно, наказать сотрудника, например, уволить его, никто не имеет права. А в случае, если это сделать, умный злоумышленник может подать в суд за нарушение его конституционных прав на личную переписку. И самое печальное, что он будет абсолютно прав. Ведь в документах не было оговорено, что вся информация, передаваемая средствами электронной почты с адресов, принадлежащих организации, является собственностью фирмы. И суд он выиграет. Руководству фирмы вряд ли понравится такая ситуация.

Можно рассмотреть вторую крайность. Этим, как правило, страдают бывшие отставные сотрудники спецслужб и армии. Что произойдет в случае, если написаны великолепные документы, но абсолютно отсутствует их техническая поддержка. Сотрудники рано или поздно нарушат правила, содержащиеся в организационных документах и, увидев, что их никто не контролирует, будут нарушать их систематически.

То есть, можно сделать вывод, что ИБ – это гибкая система, включающая как организационные, так и технические меры безопасности. При этом нужно понимать, что в безопасности нельзя выделить более или менее значимые меры. Здесь важно все. Нужно соблюдать меры защиты во всех точках сети, при работе любых субъектов с информацией. Под субъектом в данном случае понимается пользователь системы, процесс, компьютер или ПО для обработки информации. Каждый информационный ресурс, будь то компьютер пользователя или сервер организации, должен быть полностью защищен. Защищены должны быть файловые системы, сеть и так далее. Способы реализации здесь обсуждаться не будут.

Таким образом, **целью** статьи является предоставление молодым специалистам в данной области целостного алгоритма действий по созданию и внедрению отдела ИБ на предприятии.

Существует огромное количество ПО, направленного за решение задачи защиты информации. Это и антивирусные программы, и файерволы, и встроенные средства ОС. Однако стоит понять, что самым уязвимым фактором всегда остается человек. Ведь, в конце концов, работоспособность любого ПО зависит от качества его написания, от грамотности администратора, который его настроил.

Многие организации в этой связи создают отделы защиты информации или ставят задачи по ИБ перед своими ИТ-отделами. Стоит понимать, что нельзя взваливать на ИТ-службу несвойственные ей функции. Об этом не раз уже говорилось. Итак, если предположить, что в организации создан отдел ИТ-безопасности, что делать дальше? С чего начинать?

Отделу ИБ необходимо осуществить следующие шаги. Предлагается начинать с *обучения сотрудников!* И в дальнейшем сделать это регулярным процессом (не реже двух раз в год сотрудники отдела ИБ должны проходить обучение!). Обучение обычного персонала основам защиты информации должно стать постоянным делом сотрудников отдела защиты информации!

Многие руководители пытаются сразу же получить от отдела защиты информации документ под названием "Политика безопасности" [3]. Правильно ли это? Скорее нет, чем да. Ведь перед тем как сесть писать этот серьезнейший документ, который будет определять в дальнейшем все усилия по обеспечению ИБ вашей организации, нужно определиться со следующими вопросами:

Какая информация обрабатывается?

Как ее классифицировать?

Какими ресурсами вы обладаете?

Как распределена обработка информации по ресурсам?

Как классифицировать ресурсы?

Далее будет рассмотрена классификация информации. В нашей стране исторически сложился подход к классификации информации (в первую очередь, государственной) по уровням требований к ее защищенности исходя из одного свойства информации – ее конфиденциальности (секретности).

Требования к обеспечению целостности и доступности информации, как правило, лишь косвенно упоминаются среди общих требований к системам обработки этих данных.

Если такой подход в какой-то степени можно оправдать в силу необходимости обеспечения безопасности информации, составляющей государственную тайну, то это не означает, что перенос его в другую предметную область (с другими субъектами и их интересами) будет правильным.

Во многих областях доля конфиденциальной информации сравнительно мала. Для открытой информации, ущерб от разглашения которой не существен, важнейшими являются совершенно другие свойства, например, такие, как доступность, целостность или защищенность от неправомерного тиражирования. К примеру, для платежных (финансовых) документов самым важным является свойство их целостности (достоверности). Затем, по степени важности, следует свойство досту-

пности (потеря платежного документа или задержка платежей может обходиться очень дорого). Требования к обеспечению конфиденциальности платежных документов, как правило, стоят на третьем месте.

Рассмотрим следующий пример – веб-сайт Интернет-газеты. На первом месте будет стоять, по всей видимости, доступность и целостность информации, а не ее конфиденциальность.

Попытки подойти к решению вопросов защиты такой информации с позиций традиционного обеспечения только конфиденциальности, терпят провал. Основными причинами этого являются узость традиционного подхода к защите информации, отсутствие опыта и соответствующих проработок в плане обеспечения целостности и доступности информации, не являющейся конфиденциальной.

Развитие системы классификации информации по уровням требований к ее защищенности предполагает введение ряда степеней (градаций, категорий) требований по обеспечению каждого из свойств безопасности информации: доступности, целостности, конфиденциальности.

Количество дискретных градаций и вкладываемый в них смысл могут различаться.

Необходимо выделить категории защищаемой информации. Исходя из необходимости обеспечения различных уровней защиты разных видов информации (не содержащей сведений, составляющих государственную тайну), хранимой и обрабатываемой в организации, следует ввести несколько категорий конфиденциальности и несколько категорий целостности защищаемой информации.

"**Строго конфиденциальная**" – к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (банковские тайны, персональные данные), а также информация, ограничения на распространение которой введены решениями руководства организации (коммерческая тайна), разглашение которой может привести к тяжелым финансово-экономическим последствиям для организации вплоть до банкротства (нанесению значительного ущерба жизненно важным интересам его клиентов, корреспондентов, партнеров или сотрудников).

"**Конфиденциальная**" – к данной категории относится информация, не отнесенная к предыдущей категории, ограничения на распространение которой вводятся решением руководства организации в соответствии с предоставленными ему как собственнику (уполномоченному собственником лицу) информации действующим законодательством правами, разглашение которой может привести к значительным убыткам и потере конкурентоспособности организации (нанесению ощутимого ущерба интересам его клиентов, корреспондентов, партнеров или сотрудников).

"**Открытая**" – к данной категории относится информация, обеспечения конфиденциальности, введение ограничений на распространение которой не требуется.

К категориям целостности защищаемой информации можно отнести следующие:

"**Высокая**" – к данной категории относится информация, несанкционированная модификация (искажение, подмена, уничтожение) или фальсификация (подделка) которой может привести к нанесению значительного прямого ущерба организации, целостность и аутентичность (подтверждение подлинности источника) которой должна обеспечиваться гарантированными методами (средствами электронной цифровой подписи – ЭЦП) в соответствии с обязательными требованиями действующего законодательства, приказов, директив и других нормативных актов.

"**Низкая**" – к данной категории относится информация, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, ее клиентам, партнерам или сотрудникам, целостность которой должна обеспечиваться в соответствии с решением руководства (методами подсчета контрольных сумм, хеш-функций).

"**Нет требований**" – к данной категории относится информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется.

Далее рассматриваются категории функциональных задач. В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов их решения вводится четыре требуемых степени (категории) доступности функциональных задач.

"**Беспрепятственная доступность**" – доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не должна превышать нескольких секунд или минут).

"**Высокая доступность**" – доступ к задаче должен осуществляться без существенных временных задержек (задача решается ежедневно, задержка получения результата не должна превышать нескольких часов).

"**Средняя доступность**" – доступ к задаче может обеспечиваться с существенными временными задержками (задача решается раз в несколько дней, задержка получения результата не должна превышать нескольких дней).

"**Низкая доступность**" – временные задержки при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата – несколько недель).

На **первом этапе** работ производится категорирование всех видов информации, используемой при решении задач на конкретном компьютере (установление категорий конфиденциальности и целостности конкретных видов информации). Подлежащие защите информационные ресурсы включаются в "Перечень информационных ресурсов, подлежащих защите".

На **втором этапе** происходит категорирование всех функциональных задач, решаемых на данном компьютере.

На **третьем этапе** устанавливается категория компьютера, исходя из максимальных категорий обрабатываемой информации и задач, решаемых на нем.

После того, как вы смогли распределить обрабатываемую у вас информацию по соответствующим категориям, вы должны произвести инвентаризацию ресурсов.

Категорирование ресурсов. Категорирование ресурсов предполагает проведение работ по выявлению (инвентаризации) и анализу всех ресурсов подсистем автоматизированной системы (АС) организации, подлежащих защите. Примерная последовательность и основное содержание этих работ показаны ниже.

Для проведения анализа всех подсистем АС организации, проведения инвентаризации и категорирования ресурсов, подлежащих защите, формируется специальная рабочая группа. В состав этой группы включаются специалисты подразделения компьютерной безопасности и других подразделений организации (осведомленные в вопросах технологии автоматизированной обработки информации в организации).

Для придания необходимого статуса рабочей группе издается соответствующее распоряжение руководства организации, в котором, в частности, даются указания всем руководителям структурных подразделений организации об оказании содействия и необходимой помощи рабочей группе в проведении работ по анализу ресурсов всех компьютеров. Для оказания помощи на время работы группы в подразделениях руководителями этих подразделений должны выделяться сотрудники, владеющие детальной информацией по вопросам автоматизированной обработки информации в данных подразделениях.

В ходе обследования конкретных подразделений организации и автоматизированных подсистем выявляются и описываются все функциональные задачи, решаемые с использованием компьютеров, а также все виды сведений, используемые при решении этих задач в подразделениях.

Составляется общий перечень функциональных задач и для каждой задачи оформляется формуляр. При этом следует учитывать, что одна и та же задача в разных подразделениях может называться по-разному, и наоборот, различные задачи могут иметь одно и то же название. Одновременно с этим ведется учет программных средств, используемых при решении функциональных задач подразделения.

При обследовании подсистем и анализе задач выявляются все виды входящей, исходящей, хранимой, обрабатываемой и другой информации. Необходимо выявлять не только информацию, которая может быть отнесена к конфиденциальной (к банковской и коммерческой тайне, персональным данным), но и информацию, подлежащую защите в силу того, что нарушение ее целостности или доступности может нанести ощутимый ущерб организации.

При выявлении всех видов информации, циркулирующей и обрабатываемой в подсистемах, необходимо проводить оценку последствий, к которым могут привести нарушения ее свойств. Для получения первоначальных оценок таких последствий целесообразно проводить опрос (например, в форме анкетирования) специалистов, работающих с данной информацией. При этом надо выяснять, кого может интересовать данная информация, как они могут на нее воздействовать или незаконно использовать, к каким последствиям это может привести. В случае невозможности количественной оценки вероятного ущерба производится его качественная оценка (например, очень низкая, низкая, средняя, высокая, очень высокая).

При составлении перечня и формуляров функциональных задач, решаемых в организации, необходимо выяснять периодичность их решения, максимально допустимое время задержки получения результатов и степень серьезности последствий, к которым могут привести нарушения их доступности (блокирование возможности решения задач).

Все выявленные в ходе обследования различные виды информации заносятся в соответствующий документ.

Далее необходимо определить, к какому типу тайны (банковская, коммерческая, персональные данные, не составляющая тайны) относится каждый из выявленных видов информации (на основании требований действующего законодательства и предоставленных организации прав).

Первоначальные предложения по оценке категорий обеспечения конфиденциальности и целостности конкретных видов информации выясняются у руководителей (ведущих специалистов) структурного подразделения (на основе их личных оценок вероятного ущерба от нарушения свойств конфиденциальности и целостности информации). Затем Перечень согласовывается с руководителями отделов подразделений автоматизации и компьютерной безопасности и выдвигается на рассмотрение руководства организации.

На следующем этапе происходит категорирование функциональных задач. На основе требований по доступности, предъявляемых руководителями подразделений организации и согласованных со службой ИТ, категорируются все прикладные функциональные задачи, решаемые в под-

разделениях с использованием компьютерной техники. Информация о категориях специальных задач заносится в формуляры задач. Не следует проводить категорирование системных задач и программных средств вне привязки к конкретным компьютерам и прикладным задачам.

В дальнейшем с участием специалистов ИТ и подразделения ИБ необходимо уточнить состав информационных и программных ресурсов каждой задачи и внести в ее формуляр сведения по группам пользователей задачи и указания по настройке применяемых при ее решении средств защиты. Эти сведения будут использоваться в качестве эталона настроек средств защиты соответствующих компьютеров, на которых будет решаться данная задача, и для контроля правильности их установки.

На последнем этапе происходит категорирование компьютеров. Категория компьютера устанавливается, исходя из максимальной категории специальных задач, решаемых на нем, и максимальных категорий конфиденциальности и целостности информации, используемой при решении этих задач. Информация о категории компьютера заносится в его формуляр.

В понятие инвентаризации ресурсов входит не только сверка тех активных и пассивных сетевых ресурсов, которыми вы обладаете, со списком оборудования (и его комплектности), закупленного организацией. Для сверки оборудования и его комплектности можно воспользоваться соответствующим ПО, например, Microsoft SMS − сервер и так далее.

Сюда же можно отнести создание карты сети с описанием всех возможных точек подключения, списка используемого ПО, создание фонда эталонов лицензионного ПО, используемого в организации, создание фонда алгоритмов и программ собственной разработки.

Следует учесть, что ПО может быть допущено к работе лишь после его проверки отделом защиты информации на соответствие поставленным задачам и отсутствие всевозможных закладок и "логических бомб".

В этой связи хотелось бы отдельно упомянуть появившуюся в нашей стране тенденцию к использованию Open Source программного кода. Несомненно, это приносит существенную экономию ресурсов. Однако в этом случае вопрос безопасности становится вопросом доверия уже не только к разработчику системы, но и к вашему администратору. А если при этом вспомнить, сколько получает ваш администратор, то нетрудно сделать вывод, что купить ваши секреты в данном случае намного проще и дешевле, чем осуществлять прямую внешнюю атаку. Стоит упомянуть и о том, что большую часть успешных атак осуществили "инсайдеры", то есть свои же служащие компании [4].

Здесь предлагается применять свободно распространяемое ПО в случае возможности нанесения серьезного ущерба лишь тогда, если оно будет поставляться вам в откомпилированном виде и с цифровой подписью организации, гарантирующей вам отсутствие в нем логических бомб, всяческого рода закладок и "черных ходов". Причем организация-гарант должна нести материальную ответственность за свою гарантию. Однако на сегодня данное предложение можно отнести к области фантастики. Вместе с тем, конечно же, выбор за вами.

После проверки эталонное ПО заносится в фонд алгоритмов и программ (эталонная копия должна сопровождаться файлом контрольной суммы, а лучше − электронной подписью разработчика). В дальнейшем при смене версий, появлении обновлений, проверка ПО производится в установленном порядке.

Далее в формуляр каждого компьютера заносятся сведения об установленном ПО, дате установки, цели, решаемых с помощью данного ПО задачах и фамилия и подпись лица, производившего установку и настройку ПО. После создания подобных формуляров служба информационной безопасности должна обеспечивать регулярную проверку соответствия реального положения формуляру.

Таким образом, на основе представленной статьи можно получить и использовать в дальнейшем руководство для молодых специалистов в области ИБ, на основе которого формировать необходимую полноценную организационно-штатную структуру предприятия в виде соответствующего отдела ИБ со своими функциональными обязанностями.

Следующим этапом в построении службы защиты информации (или отдела ИБ) должен являться анализ рисков организации, из которого будет вытекать создание политики безопасности, чему и необходимо посвятить дальнейшие исследования.

Литература: 1. Куприянов А. И. Основы защиты информации / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М.: Изд. центр "Академия", 2006. – 256 с. 2. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков – К.: Юниор, 2003. – 504 с. 3. Кавун С. В. Методика построения политики безопасности организации / С. В. Кавун, Г. В. Шубина // Бизнес Информ. – 2005. – №1–2 – С. 96 – 102. 4. Кавун С. Организация противодействия инсайдерам в предпринимательской деятельности // Економіка розвитку. – 2008. – №1(45). – С. 9 – 11.

Секція 2
Захист інформації в комп'ютерних системах

Кузнецов А. А.

Король О. Г.

Ткачов А. М.

УДК 336.717:004.78

АНАЛИЗ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАНКОВСКОЙ ИНФОРМАЦИИ ВО ВНУТРИПЛАТЕЖНЫХ СИСТЕМАХ КОММЕРЧЕСКОГО БАНКА

Развитие экономики любого государства сегодня невозможно без высокоэффективной системы денежного обращения и использования современных платежных механизмов. Процесс развития рыночной экономики требует наличия соответствующей платежной системы, позволяющей осуществлять расчеты в народном хозяйстве в соответствии с общепринятыми мировыми стандартами. В этой связи на первый план выходят надежность, безопасность, а также срочность осуществления платежей.

Национальная платежная система – сложная многоуровневая система централизованного управления, обеспечивающая качественный стратегически важный канал проведения финансовых транзакций [1].

Такая система относится к сложным многоуровневым системам управления критического применения (СУКП), в которых передача информации требует контроля безопасности на каждом уровне [1]. Основными элементами системы являются система электронных платежей (СЭП) и внутриплатежная система коммерческого банка (ВПС КБ). Структурная схема СУКП национальной платежной системы представлена на рис. 1.

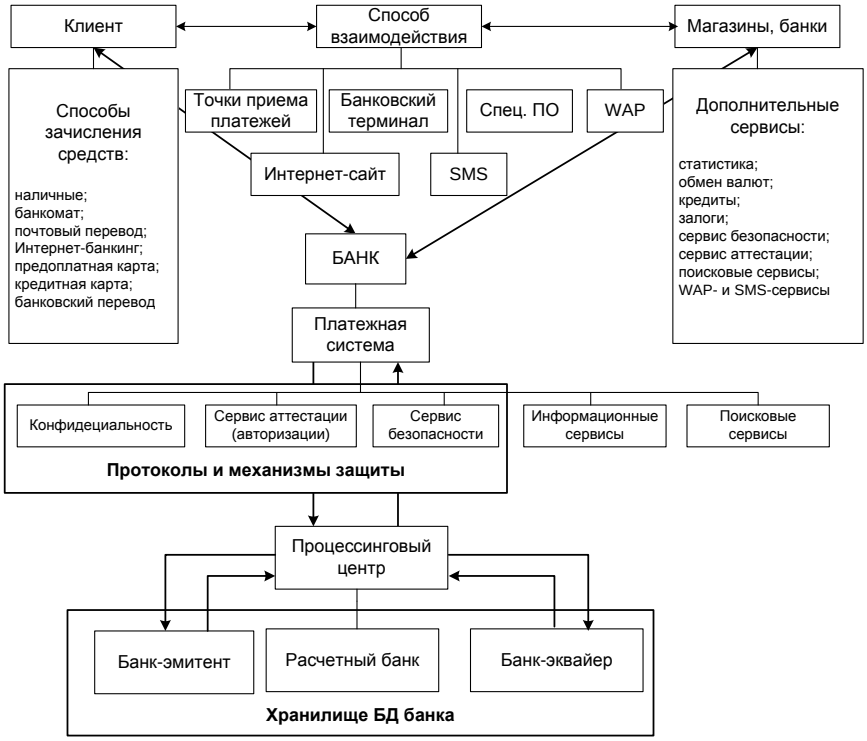


Рис. 1. **Структурная схема национальной платежной системы**

Эффективность функционирования каждого из элементов зависит от быстродействия и надежности используемых механизмов аутентификации. Практически любая современная банковская система не обходится без использования механизмов шифрования и обеспечения аутентичности информации.

Тем не менее, на сегодняшний день не существует научно обоснованной концепции и механизмов обеспечения финансовой безопасности банковской деятельности национальной платежной системы в целом [2]. Новизна и актуальность проблем обеспечения безопасности банковской деятельности привлекают внимание ученых, среди которых: В. Ю. Гайкович, А. Ю. Першин, М. И. Анохин, Н. П. Варновский, В. М. Сидельников, В. В. Ященко [3; 4]. и др. Среди зарубежных авторов — S. D. Galbraith, N. P. A. Smart, M. O. Rabin, B. Столлингс [5 – 7]. Современные подходы к обеспечению экономической и финансовой безопасности банковской деятельности, обеспечению их надежности и устойчивости представили в своих работах Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин [8]. Проведенный обзор работ в данном направлении показал, что проблемными вопросами в открытых системах, в том числе и ВПС КБ, являются вопросы обеспечения аутентичности и целостности открытых ключей. Однако результаты этих работ позволяют выбрать механизмы обеспечения безопасности информации, отвечающие требованиям к стойкости и вычислительной сложности криптопреобразований лишь на определенное время.

Известным приемом в построении современных механизмов аутентификации является использование стойких криптопримитивов, например, схемы UMAC, TTMAC, HMAC и др. Подход, используемый в данных схемах, позволил свести стойкость схем аутентификации к стойкости используемого алгоритма (DES, TDES, AES), что также не решило возникшей проблемы. Следовательно, современной и востребованной задачей, позволяющей решить существующие противоречия при выборе механизмов аутентификации и оценки их стойкости, является проведение анализа криптографической стойкости существующих криптопримитивов и разработка рекомендаций по обоснованию стойкости современных систем аутентификации.

Цель статьи – рассмотрение основных механизмов обеспечения безопасности во внутриплатежных системах коммерческого банка (ВПС КБ), проведение анализа угроз и механизмов обеспечения аутентичности, целостности банковской информации в ВПС КБ.

В развитии рыночных отношений и формировании коммерческих структур главенствующую роль играют коммерческие банки, аккумулирующие огромные финансовые потоки. Это привлекает огромный интерес криминальных структур, спецслужб и конкурентов. Основная угроза при этом ложится именно на ВПС КБ [9]. В связи с этим проблема безопасности национальной платежной системы (обеспечение аутентичности, целостности и конфиденциальности всех проводимых электронных операций) остается нерешенной.

Рассмотрим основные составляющие национальной платежной системы.

Система электронных платежей (СЭП) – комплекс аппаратных и программных средств, производящих оплату товаров посредством компьютерных или магнитных карточек, предназначенных для создания основы электронных денег, перспективной альтернативы методам оплаты наличными деньгами и чеками [10]. На рис. 2 представлена обобщенная структурная схема электронной платежной системы.

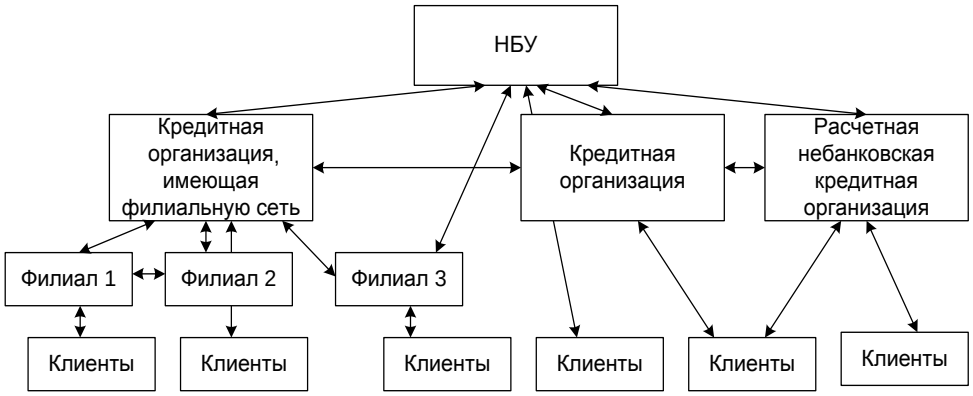


Рис. 2. **Обобщенная структурная схема электронной платежной системы**

Банк, заключивший соглашение с платежной системой и получивший соответствующую лицензию, может выступать в двух качествах – как банк-эмитент и как банк-эквайер. Банк-эмитент выпускает пластиковые карты и гарантирует выполнение финансовых обязательств, связанных с использованием этих карт как платежных средств. Банк-эквайер обслуживает предприятия торговли и сервиса, принимающие к оплате карты как платежные средства, а также принимает эти платежные средства к обналичиванию в своих отделениях и через принадлежащие ему банкоматы. Основными неотъемлемыми функциями банка-эквайера являются финансовые операции, связанные с выполнением расчетов и платежей точками обслуживания. Технические атрибуты деятельности банка-эквайера (обработка

запросов на авторизацию; перечисление на расчетные счета точек средств за товары и услуги, предоставленные по картам; прием, сортировка и пересылка документов, фиксирующих совершение сделок с использованием карт и т. п.) могут быть делегированы эквайером процессинговым центрам и связаны с обеспечением защиты передаваемых данных [8].

Данная система интегрируется в банковские системы и множество типов терминалов, в том числе переносные, работающие в автономном режиме, и банкоматы, выполняющие более широкий спектр функций. СЭП управляет потоками электронных денег, связью терминалов и локальных сетей.

Для обеспечения надежной работы электронная платежная система должна быть надежно защищена. С точки зрения информационной безопасности в СЭП существуют следующие уязвимые места:

пересылка платежных и других сообщений между банком и клиентом и между банками;

обработка информации внутри организаций отправителя и получателя сообщений;

доступ клиентов к средствам, аккумулированным на счетах.

Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом. Пересылка платежных и других сообщений связана со следующими особенностями:

внутренние системы организаций отправителя и получателя должны быть приспособлены для отправки и получения электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

взаимодействие отправителя и получателя электронного документа осуществляется опосредовано через канал связи.

Эти особенности порождают следующие *проблемы*:

взаимное опознавание абонентов (проблема установления взаимной подлинности при установлении соединения);

защита электронных документов, передаваемых по каналам связи (проблемы обеспечения конфиденциальности и целостности документов);

защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);

обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости) [3].

Для обеспечения функций защиты информации на отдельных узлах системы должны быть реализованы следующие *услуги защиты* [8]:

управление доступом на оконечных системах;

контроль целостности сообщения;

обеспечение конфиденциальности сообщения;

взаимная аутентификация абонентов;

причастность к формированию сообщения;

гарантии доставки сообщения;

причастность к получению сообщения;

регистрация последовательности сообщений;

контроль целостности последовательности сообщений.

Качество решения указанных выше проблем в значительной мере определяется рациональным выбором криптографических средств при реализации механизмов защиты (рис. 3).

Рис. 3. **Механизмы защиты**

Внутриплатежная система коммерческого банка обеспечивает реализацию функций обработки платежных документов (прием от филиалов файлов начальных платежей; контроль начальных платежей СЭП, формирование и отправка файлов начальных платежей в АРМ-СЭП; прием от АРМ-СЭП файлов ответных платежей; отправка файлов ответных платежей на филиалы), управление филиалами-участниками ВПС (установка лимитов корсчетов филиалов в ВПС; блокировка начальных и ответных платежей филиалов), взаимодействие с информационно-поисковой системой

(ИПС) НБУ, а также работа внутренней ИПС. Сравнение функциональных возможностей и механизмов защиты современных ВПС представлены в табл. 1.

Таблица 1

Сравнение функциональных возможностей современных ВПС

Системы электронных платежей банка	Функции системы	Уровни применения механизмов защиты
ВПС "ГРАНТ" – предназначена для выполнения платежей в национальной валюте Украины между головным банком и его филиалами, а также платежей в СЭП НБУ головным банком и его филиалами	Обработка платежных документов; защита информации; управление филиалами-участниками ВПС; взаимодействие с информационно-поисковой системой (ИПС) НБУ, а также работа внутренней ИПС	Уровень защищенной операционной среды; уровень СУБД; уровень прикладного программного обеспечения; уровень средств криптографической защиты информации
Enigma – обеспечивает автоматизацию внутрибанковских и межбанковских платежей в многофилиальных банках Украины	Обмен пакетами документов и технологическими файлами между головным банком, филиалами и системой электронных платежей НБУ; наложение логических и бухгалтерских ограничений на различные платежные операции в СЭП НБУ, ВПС и АБС банка	Уровень средств криптографической защиты информации
ProFIX/TELEBANK – предназначена для управления ресурсами многофилиального банка	Обработка входящих и исходящих сообщений; проведение ручных утверждений сообщений, поступающих на исполнение от служб и филиалов; предоставление услуг другим банкам в качестве клирингового банка	Система обладает встроенными механизмами обеспечения безопасности электронных платежей, которые построены по принципам и форматам СЭП; используется система шифрования на базе алгоритма DES и электронной подписи на базе алгоритма RSA
Внутрибанковская платежная система (ВПС) — новый программный продукт, разработанный специалистами компании R-Style Ukraine, предназначенный для управления финансовыми потоками в многофилиальном банке	Принятие от филиала-отправителя внутрибанковского платежа и доставить его через расчетный центр в филиал-получатель; выполнение всех операций по учету движения средств, предусмотренные выбранной бухгалтерской моделью, обеспечивает корректность консолидированного баланса банка и гарантирует целостность данных и защиту информации	Уровень защищенной операционной среды уровень СУБД; уровень прикладного программного обеспечения; уровень средств криптографической защиты информации;

Несмотря на широкое применение различных криптографических алгоритмов на различных уровнях защиты, внутриплатежные системы подвержены различным атакам и угрозам, подразделяемым на угрозы *финансовых ресурсов*, так называемая чувствительная информация: персональная информация пользователей – (имена, пароли, аккаунты, идентификационные номера, банковские реквизиты, данные о корпоративных сетях, (с помощью такого рода сведений возможен обход многоуровневых систем защиты от вторжений), и угрозы *информационных ресурсов*, которые подразделяются на внешние (технические) и внутренние (неправомерные действия сотрудников). На рис. 4 представлены основные типы угроз информационных ресурсов [11].

Рис. 4. **Основные типы угроз информационных ресурсов**

Наиболее уязвима инфраструктура безопасности крупных банков. Большое количество сотрудников, множество компьютеров, разнородные сети и права доступа − эти дополнительные факторы облегчают задачу злоумышленникам [12].

Сегодня внутренние угрозы являются одной из наиболее актуальных проблем информационной безопасности. Согласно статистике, неправомерные действия сотрудников самих организаций причиняют наибольший ущерб и до 90% средств, выделяемых на информационную безопасность, тратится на обеспечение защиты от внутренних атак [12].

Неправомерные действия пользователей приводят к значительному ущербу и подразделяются:

нарушение конфиденциальности данных;

кража информации;

искажение информации;

действия, приводящие к сбоям информационных систем;

утрата информации.

Лидирующую позицию занимают нарушения конфиденциальности данных, приводящие к утечке закрытой информации. По сведениям специалистов [12], из 100 случаев неправомерных действий сотрудников 65 относятся к нарушению конфиденциальности данных. Диаграмма распределения внутренних угроз представлена на рис. 5.

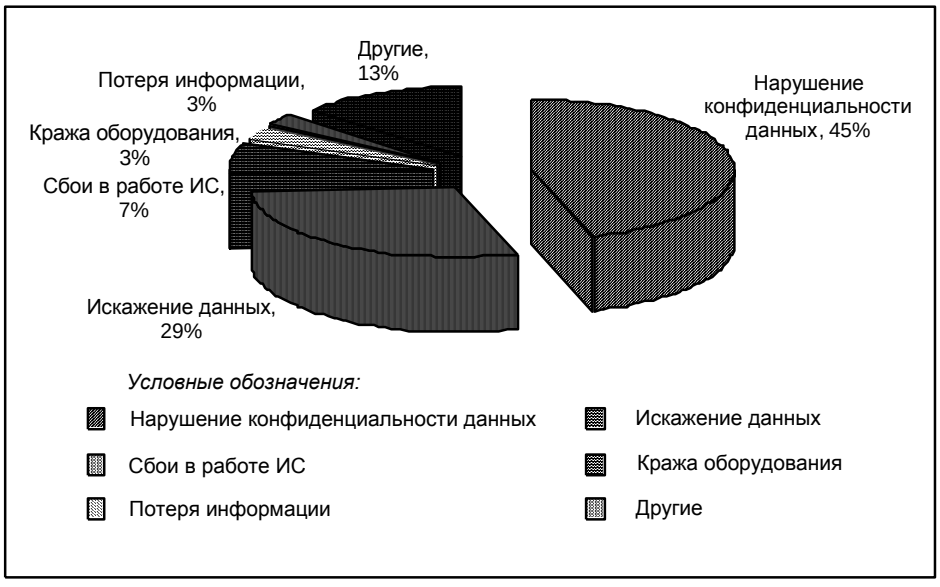


Рис. 5. **Диаграмма распределения внутренних угроз**

Самыми распространенными путями утечки информации являются электронная почта (до 22%), Интернет (сайты, чаты, форумы, бесплатные почтовые сервисы) — до 20%, Интернет-пейджеры (ICQ/AOL, AIM, MSN, Yahoo!) и мобильные накопители (компакт-диски, USB-

накопители) — до 19%, печатающие устройства − до 8% и другие источники — до 12%. Диаграмма утечки конфиденциальной информации представлена на рис. 6.

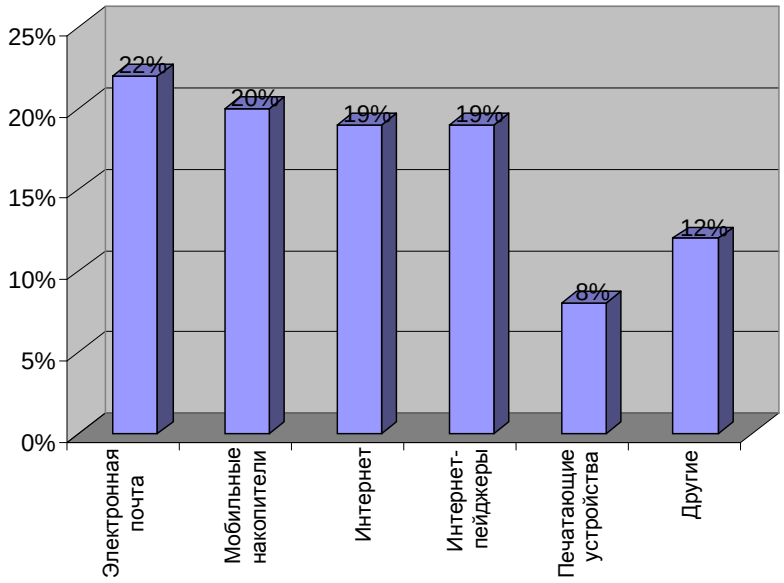


Рис. 6. **Диаграмма утечки конфиденциальной информации**

Для обеспечения защиты от рассмотренных угроз используются различные криптографические механизмы. ВПС КБ имеет собственную систему защиты информации, отвечающую требованиям НБУ.

Система защиты информации ВПС КБ должна обеспечивать высокий уровень информационной безопасности банка на каждом этапе подготовки, обработки и выполнения электронных банковских документов на всех уровнях за счет положенного в ее основу комплексного подхода к проблеме обеспечения защиты.

Создание защищенной среды обработки информации реализуется на нескольких уровнях [13]:

первый − уровень защищенной операционной среды (ОС), обеспечивающей авторизованный доступ к файлам, каталогам и программам в отдельности на чтение, модификацию и запуск и удовлетворяющей общепризнанному в мире уровню безопасности;

второй − уровень системы управления базами данных (СУБД), обеспечивающей авторизованный доступ к информации в базе данных в отдельности на чтение, пополнение и модификацию, а также автоматическое ведение протокольных журналов работы пользователей;

третий − уровень прикладного программного обеспечения ВПС КБ и СЭП, на котором реализованы подсистемы:

внутреннего аудита, протоколирующая все изменения состояния платежных документов;

разграничения доступа к информации и управления правами пользователей, являющаяся логическим продолжением механизмов СУБД и обеспечивающая предоставление каждому пользователю строго регламентированного набора полномочий как на выполнение тех или других операций, так и на доступ к соответствующей части информации БД;

четвертый − уровень средств криптографической защиты информации на базе программных средств криптографической защиты информации (КЗИ), обеспечивающих:

наложение/проверку цифровой подписи (ЦП) на все платежные документы;

наложение/проверку ЦП на все платежные и служебные файлы;

шифрование циркулирующей информации;

управление ключами ЦП пользователей СЭП.

Основные механизмы аутентичности, целостности информации в ВПС КБ на различных уровнях (между филиалами, отделениями, центрами и терминалами) и информации, циркулирующей в банковской системе, основаны на использовании стандартов блочно-симметричных шифров (DES, ГОСТ 28147-89 (4 режим)) [14 — 17].

Примером программной реализации рассмотренных механизмов аутентичности являются программные средства криптографической защиты информации "Грифон-Б" и "Грифон-Л", разработанные ООО СНПФ "АРГУС". Программное средство "Грифон-Б" предназначено для криптографической защиты конфиденциальной информации в автоматизированных банковских системах и применяется для обмена информацией внутри корпоративной сети банка, с клиентами, работающими по системе "Клиент-Банк", в системах обслуживания пластиковых карт [13].

Программное средство криптографической защиты информации "Грифон-Л" [18] предназначено для использования в сфере банковской деятельности, в частности, для обмена конфиденциальной (в том числе финансовой) информацией внутри корпоративной сети банка, с клиентами,

работающими по системе "Клиент-Банк", в системах обслуживания пластиковых карт и пр. Основные технические характеристики данных программных средств защиты приведены в табл. 2.

Таблица 2

Основные характеристики программных средств защиты

№ п/п	Сравнительные характеристики	"Грифон-Б"	"Грифон-Л"
1	Обеспечение реализации криптоалгоритмов	Криптографическое преобразование в соответствии с ГОСТ 28147-89 в режимах простой замены, гаммирования и гаммирования с обратной связью для областей памяти и файлов; формирование иммитовставки длиной 32 бит в соответствии с ГОСТ 28147-89; хеширование в соответствии с ГОСТ 34.311-95 для областей памяти и файлов; генерация секретного ключа электронной цифровой подписи *x*, секретного параметра *k* для реализации ГОСТ 34.310-95, а также генерация сеансовых ключей для реализации ГОСТ 28147-89; генерация открытой ключевой информации, вычисление и проверка электронной цифровой подписи на базе асимметричного криптографического алгоритма в соответствии с ГОСТ 34.310-95 для областей памяти и файлов; распределение сеансовых ключей в соответствии с протоколом обмена ключами на основе алгоритма Диффи – Хеллмана	Криптографическое преобразование в соответствии с ГОСТ 28147-89 в режимах простой замены, гаммирования и гаммирования с обратной связью; формирование иммитовставки длиной 32 бит, в соответствии с ГОСТ 28147-89; хеширование в соответствии с ГОСТ 34.311-95; формирование системных параметров, вычисление и проверка электронной цифровой подписи (ЕЦП) на базе асимметричного криптографического алгоритма в соответствии с ГОСТ 34.310-95; генерация секретного ключа электронной цифровой подписи *x*, секретного параметра *k* для реализаций ГОСТ 34.310-95, а также генерация сеансовых ключей для реализации ГОСТ 28147-89; генерация случайных чисел, которые имеют статистические характеристики, допускающие их использование в качестве ключевых данных для криптографических преобразований в соответствии с алгоритмами ГОСТ 28147-89, ГОСТ 34.310-95; формирование ключей защиты сеансовых ключей в соответствии с протоколом асимметричного распределения ключей типа Диффи – Хеллмана
2	Основные функции программы	Получение справочной информации. Тест хеширования, в том числе шифрования простой заменой. Получение чисел p, q (512 бит и 1024 бит). Тест создания и проверки ЭЦП. Тесты быстродействия (шифрования, хеширования, генерации чисел, наложения подписи и др.). Простое и адресное шифрование строки или файла. Хеширование строки или файла. Генерация общесистемных параметров. Генерация макета ключа пользователя. Генерация ключа пользователя. Смена пароля на секретном ключе. Подпись строки или файла. Проверка подписи. Снятие подписи. Общий секретный ключ Z AB по Диффи – Хеллману	
3	Применяемые стандарты	ГОСТ 28147-89. Алгоритм криптографического преобразования. ГОСТ 34.311-95. Функция хеширования. ГОСТ 34.310-95. Процедура выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма. Кроме того, использованы схема распределения симметричных ключей Диффи – Хеллмана и стандарт X9.17 для генерации сеансовых ключей	
4	Быстродействие на ПК с процессором 633 МГц обеспечивает	Шифрование области памяти в режиме простой замены – не менее 5 Мб/с; хеширование области памяти – не менее 1,5 Мб/с; вычисление электронной цифровой подписи при длине ключа 512 бит – не более 0,015 с; проверка электронной подписи при длине ключа 512 бит – не более 0,020 с; генерацию общего ключа по методу Диффи – Хеллмана при длине ключа 512 бит – не более 0,015 с	Шифрование области памяти в режиме простой замены – не менее 2,5 Мб/с; хеширование области памяти – не менее 1 Мб/с; вычисление электронной цифровой подписи при длине ключа 512 бит – не более 0.020 с; проверку электронной подписи при длине ключа 512 бит – не более 0,030 с; генерацию общего секретного ключа при длине открытой составляющей ключа 512 бит – не более 0,020 с

Проверка работоспособности данных программ выполняется с помощью встроенных функций самоконтроля. Поставляются программы с интерфейсом командной строки в нескольких модификациях: для выполнения тестовых примеров, проверки быстродействия базовых алгоритмов, выполнения функций генерации ключей, а также выполнения основных операций, необходимых пользователю (шифрование, цифровая подпись и др.) [13; 18].

Таким образом, проведенные исследования показали, что для обеспечения безопасности банковской информации в ВПС КБ используются криптографические симметричные и асимметрические алгоритмы шифрования, обеспечивающие аутентичность и целостность сообщений. Вместе с тем некоторые криптографические функции не обеспечивают требуемой защиты без специальных секретов кодов подтверждения подлинности, которые должны представлять дополнительный механизм обработки исходного или шифрованного текста (ЭЦП, хэш-функции), и являются эффективными для больших объемов потоков данных и не удовлетворяют требованиям к современным системам управления критического применения (ВПС КБ).

Литература: 1. http://www. cryptopro. ru/cryptopro/documentation/dig-cert. htm 2. Артеменко Д. А. Механизм обеспечения финансовой безопасности банковской деятельности: Дис. канд. экон. наук. – Ростов н/Д:, Б. и., 1999. – 190 с. 3. Гайкович В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович, А. Ю. Першин. — М.: Ед. Европа, 1994. – 286 с. 4. Логинов А. А. Общие принципы функционирования электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества / А. А. Логинов, Н. С. Елхимов // Конфидент. — 1995. — №4. — С. 48 – 54. 5. Rabin M. O. Fingerprinting by Random Polynomials // Tech. Rep. TR-15-81, Center: in Compating Technology, Harvard Univ., Cambridge, Mass., 1981. 6. Столлингс В. Криптография и защита сетей: принципы и практика: Пер. с англ. – 2-е изд. — М.: Изд. дом "Вильямс", 2001. — 672 с. 7. Шефановский Д. Б. ГОСТ 34.11 – 94. Функция хэширования. Краткий анализ. — М.: Учебн. центр "Инфозащита", 2001. — 18 с. 8. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; [Под ред. В. Ф. Шаньгина. — 2-е изд., перераб. и доп. — М.: Радио и связь, 2001. – 376 с. 9. Межбанковские расчеты на Украине // http://e2000.kyiv. org/biblioteka/biblio/stat/ukr_bank. html 10. http://www. carteblanche-online. info/index. php?option =com_ content&task =view&id=105 11. Вихорев С. В. Классификация угроз информационной безопасности // http:// www2. cnews. ru/comments/security/elvis_class. shtml 12. http://www. jetinfo. ru/2005/10/1/article1. 9. 200518. html 13. Программное средство криптографической защиты информации "Грифон-Б" // http://www. banksoft. com. ua/index. php?id=28 14. ГОСТ 34.310-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. — К.: Госстандарт Украины, 1998. — 68 с. 15. ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хеширования. – К.: Госстандарт Украины, 1998. — 46 с. 16. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма – М.: МИФИ, 1995. – 16 с. 17. Анохин М. И. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. Криптография в банковском деле / М. И. Анохин, Н. П. Варновский, В. М. Сидельников, В. В. Ященко. – М.: МИФИ, 1997. — 274 с. 18. Программное средство "Библиотека функций криптографической защиты информации "Грифон-Л" // http://www. banksoft. com. ua/index. php?id=27

УДК 336.717:004.78

Купрейчик И. В.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречен на бесконечность в своей последовательности. Хотя, если уж быть точным, новые проблемы − это всего лишь обновленная форма старых. Вечная проблема − защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине XX века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества.

Главная тенденция, характеризующая развитие современных информационных технологий − рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированным доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте.

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются: переход от традиционной "бумажной" технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях; объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам; увеличение сложности программных средств и связанное с этим уменьшение их надежности и увеличение числа уязвимостей.

Любое современное предприятие независимо от вида деятельности и формы собственности не в состоянии успешно развиваться и вести хозяйственную деятельность без создания на нем условий для надежного функционирования системы защиты собственной информации.

Отсутствие у многих руководителей предприятий и компаний четкого представления по вопросам защиты информации приводит к тому, что им сложно в полной мере оценить необходимость создания надежной системы защиты информации на своем предприятии и тем более сложно бывает определить конкретные действия, необходимые для защиты тех или иных конфиденциальных сведений [1].

Отрицательную роль при этом играют и некоторые средства массовой информации, публикуя "панические" статьи о состоянии дел по защите информации, формирующие у читателей представление о невозможности в современных условиях обеспечить требуемый уровень защиты информации. Можно с уверенностью утверждать, что создание эффективной системы защиты информации сегодня вполне реально. Надежность защиты информации, прежде всего, будет определяться полнотой решения целого комплекса задач, речь о которых будет продолжена дальше.

Современные компьютерные системы, использующие операционные системы (ОС) Windows, Windows NT, различные версии UNIX относятся к частично контролируемым системам. Неприятной особенностью таких ОС является то, что полный перечень всех их возможностей полностью не известен пользователю. Резонно допустить наличие в этих ОС скрытых возможностей осуществления несанкционированного доступа к информации, обрабатываемой под их управлением.

Такие скрытые возможности могут появиться как в результате ошибки или действий недобросовестных разработчиков, так и в соответствии с "техническим заданием". Их наличие подтверждают исследования австралийской компании Shake Communication Pty Ltd, выявившие более сотни уязвимых мест в программном обеспечении Microsoft Windows NT.

Рассмотрим вариант существования таких скрытых возможностей в виде "программных закладок" в поставляемых лицензионных ОС. "Программные закладки", внедренные в лицензионную ОС на этапе ее эксплуатации, нарушают ее целостность и поэтому могут быть обнаружены. Конечно, проверка целостности ОС должна осуществляться полностью контролируемыми средствами, а не приложением, работающим в этой же ОС. Закладки же внутри ОС с помощью проверки целостности обнаружить невозможно.

Какими возможностями может обладать внедренная на этапе разработки ОС "программная закладка"? В отличие от пользователя для разработчика ОС последняя является полностью контролируемой средой. Поэтому он может реализовать закладку практически с неограниченными возможностями. Рассмотрим несколько возможных вариантов:

1. Закладки, позволяющие обойти, отключить, модифицировать стандартные средства ОС для разграничения доступа и интерфейс для подключения пользовательского шифрования. Разработка такой закладки не должна быть сложной.

2. Закладки, перехватывающие информацию по любому из прерываний и портам и складирующие ее в скрытые или неиспользуемые зоны жесткого диска (отформатированный стандартными средствами диск вполне может иметь такие зоны). В дальнейшем эта информация может предоставляться для анализа злоумышленнику или отправляться по сети другими закладками. С помощью такой закладки можно перехватывать не только обычную информацию, но и пароли, вводимые с клавиатуры, или поступающие по другим стандартным интерфейсам.

3. Закладки, обеспечивающие доступ в оперативную память любого приложения. Анализ перехваченной из оперативной памяти информации совместно с кодом приложения может использоваться для перехвата ключей шифрования и ЭЦП в оперативной памяти.

4. Закладки, обеспечивающие прямой выход в сеть, для отправки перехваченной информации в обход описанных в документации средств. Они могут работать навстречу друг другу и совсем не по описанным в документации протоколам.

Перечисленных выше вариантов вполне достаточно, чтобы нейтрализовать известные ныне отечественные средства защиты информации для компьютерных систем, работающих под перечисленными выше ОС. Однако уж очень заманчиво, сосредоточив в руках одной фирмы или одного государства рынок аппаратных и программных средств, попытаться осуществить тотальный контроль за обрабатываемой этими средствами информацией. Тем более, что реализовать набор средств для перехвата в составе ОС и в аппаратуре не так уж сложно.

Защищают информацию в частично контролируемых системах традиционные средства:

абонентское шифрование;

"прозрачное" шифрование информации в TCP/IP сетях;

"прозрачное" шифрование логических и сетевых дисков;

межсетевые экраны;

программно-аппаратные системы защиты от несанкционированного доступа (ЗНСД).

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

В настоящее время отсутствует какая-либо универсальная методика, позволяющая четко соотносить ту или иную информацию к категории коммерческой тайны. Можно только посоветовать исходить из принципа экономической выгоды и безопасности предприятия – чрезмерная "засекреченность" приводит к необоснованному подорожанию необходимых мер по защите информации и не способствует развитию бизнеса, когда широкая открытость может привести к большим финансовым потерям или разглашению тайны.

Определившись в необходимости защиты информации, непосредственно приступают к проектированию системы защиты информации.

Конкретное содержание указанных мероприятий для каждого отдельно взятого предприятия может быть различным по масштабам и формам. Это зависит в первую очередь от производственных, финансовых и иных возможностей предприятия, от объемов конфиденциальной информации и степени ее значимости. Существенным является то, что весь перечень указанных мероприятий обязательно должен планироваться и использоваться с учетом особенностей функционирования информационной системы предприятия.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации.

Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий сохранности конфиденциальной информации. Необходимо четко определять круг сотрудников, допускаемых к конфиденциальной информации, к каким конкретно сведениям им разрешен доступ и полномочия сотрудников по доступу к конфиденциальной информации. Как показывает практика работы, для разработки необходимого комплекса мероприятий по защите информации желательно привлечение квалифицированных экспертов в области защиты информации.

Традиционно для организации доступа к конфиденциальной информации использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами. Однако с развитием компьютерных систем эти меры перестали обеспечивать необходимую безопасность информации. Появились и в настоящее время широко применяются специализированные программные и программно-аппаратные средства защиты информации, которые позволяют максимально автоматизировать процедуры доступа к информации и обеспечить при этом требуемую степень ее защиты. Подробнее о существующих средствах защиты информации остановимся ниже. Осуществление контроля за соблюдением установленного режима конфиденциальности предусматривает проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации. Как правило, контроль осуществляется в виде плановых и внеплановых проверок силами своих сотрудников или с привлечением других организаций, которые специализируются в этой области.

По результатам проверок специалистами по защите информации проводится необходимый анализ с составлением отчета, который включает: вывод о соответствии проводимых на предприятии мероприятий установленным требованиям; оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

Обеспечение и реализация перечисленных выше мероприятий потребует создания на предприятии соответствующих органов защиты информации. Эффективность защиты информации на предприятии во многом будет определяться тем, насколько правильно выбрана структура органа защиты информации и квалифицированны его сотрудники. Как правило, органы защиты информации представляют собой самостоятельные подразделения, однако на практике часто практикуется и назначение одного из штатных специалистов предприятия ответственным за обеспечение защиты информации.

Однако такая форма оправдана в тех случаях, когда объем необходимых мероприятий по защите информации небольшой и создание отдельного подразделения экономически не выгодно.

Созданием органов защиты информации на предприятии завершается построение системы защиты информации, под которой понимается совокупность органов защиты информации или отдельных исполнителей, используемые ими средства защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Как уже отмечалось выше, эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;

средства, обеспечивающие защиту информации при передаче ее по каналам связи;

средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;

средства, обеспечивающие защиту от воздействия программ-вирусов;

материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Основное назначение средств защиты первой группы – разграничение доступа к локальным и сетевым информационным ресурсам автоматизированных систем. СЗИ этой группы обеспечивают: идентификацию и аутентификацию пользователей автоматизированных систем; разграничение доступа зарегистрированных пользователей к информационным ресурсам;

регистрацию действий пользователей; защиту загрузки операционной системы с гибких магнитных дисков и CD-ROM; контроль целостности СЗИ и информационных ресурсов.

В качестве идентификаторов пользователей применяются, как правило, условные обозначения в виде набора символов. Для аутентификации пользователей применяются пароли. Ввод значений идентификатора пользователя и его пароля осуществляется по запросу СЗИ с клавиатуры. Многие современные СЗИ используют и другие типы идентификаторов – магнитные карточки, радиочастотные бесконтактные карточки, смарт-карточки, электронные таблетки Touch Memory и др. Отдельно стоит сказать об использовании в качестве идентификатора индивидуальных биологических параметров (отпечаток пальца, радужная оболочка глаза), присущих каждому человеку. Использование в качестве идентификаторов индивидуальных биологических параметров характеризуется, с одной стороны, высшим уровнем конфиденциальности, а с другой – очень высокой стоимостью таких систем.

Разграничение доступа зарегистрированных пользователей к информационным ресурсам осуществляется СЗИ в соответствии с установленными для пользователей полномочиями. Как правило, СЗИ обеспечивают разграничение доступа к гибким и жестким дискам, логическим дискам, директориям, файлам, портам и устройствам. Полномочия пользователей устанавливаются с помощью специальных настроек СЗИ. По отношению к информационным ресурсам средствами защиты могут устанавливаться такие полномочия, как разрешение чтения, записи, создания, запуска исполняемых файлов и другие. Системы защиты информации предусматривают ведение специального журнала, в котором регистрируются определенные события, связанные с действиями пользователей, например запись (модификация) файла, запуск программы, вывод на печать и другие, а также попытки несанкционированного доступа к защищаемым ресурсам и их результат.

Особо стоит отметить наличие в СЗИ защиты загрузки операционной системы с гибких магнитных дисков и CD-ROM, которая обеспечивает защиту самих средств защиты от "взлома" с использованием специальных технологий. В различных СЗИ существуют программные и аппаратно-программные реализации этой защиты, однако практика показывает, что программная реализация не обеспечивает необходимой стойкости.

Контроль целостности средств защиты и защищаемых файлов заключается в подсчете и сравнении контрольных сумм файлов. При этом используются различной сложности алгоритмы подсчета контрольных сумм. Несмотря на функциональную общность средств защиты информации данной группы, СЗИ различных производителей различаются: условиями функционирования (операционная среда, аппаратная платформа, автономные компьютеры и вычислительные сети); сложностью настройки и управления параметрами СЗИ; используемыми типами идентификаторов; перечнем событий, подлежащих регистрации; стоимостью средств защиты.

С развитием сетевых технологий появился новый тип СЗИ – межсетевые экраны (firewalls), которые обеспечивают решение таких задач, как защита подключений к внешним сетям, разграничение доступа между сегментами корпоративной сети, защита корпоративных потоков данных, передаваемых по открытым сетям.

Защита информации при передаче ее по каналам связи осуществляется средствами криптографической защиты (СКЗИ). Характерной особенностью этих средств является то, что они потенциально обеспечивают наивысшую защиту передаваемой информации от несанкционированного доступа к ней. Помимо этого СКЗИ обеспечивают защиту информации от модификации (использование цифровой подписи и имитовставки).

Как правило, СКЗИ функционируют в автоматизированных системах как самостоятельное средство, однако в отдельных случаях СКЗИ может функционировать в составе средств разграничения доступа как функциональная подсистема для усиления защитных свойств последних.

Обеспечивая высокую степень защиты информации, в то же время применение СКЗИ влечет ряд неудобств: стойкость СКЗИ является потенциальной, то есть гарантируется при соблюдении ряда дополнительных требований, реализация которых на практике осуществляется довольно сложно (создание и функционирование ключевой системы, распределение ключей, обеспечение сохранности ключей, необходимость в получении лицензии ФАПСИ на право эксплуатации средств, планирование и организация мероприятий при компрометации ключевой системы); относительно высокая стоимость эксплуатации таких средств.

В целом, при определении необходимости использования средств криптографической защиты информации, необходимо учитывать то, что применение СКЗИ оправдано в случаях явного перехвата действительно конфиденциальной информации.

Целью статьи не является широкое обсуждение средств защиты от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем, однако отметим, что для защиты информации от утечки по физическим полям исполь-

зуются следующие методы и средства защиты: электромагнитное экранирование устройств или помещений, в которых расположена вычислительная техника; активная радиотехническая маскировка с использованием широкополосных генераторов шумов, которые широко представлены на нашем рынке.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако этот способ требует значительных капитальных затрат и практически не применяется.

И несколько слов о материалах, обеспечивающих безопасность хранения, транспортировки носителей информации и защиту их от копирования. В основном это специальные тонкопленочные материалы с изменяющейся цветовой гаммой или голографические метки, которые наносятся на документы и предметы (в том числе и на элементы компьютерной техники автоматизированных систем). Они позволяют: идентифицировать подлинность объекта; контролировать несанкционированный доступ к ним.

Широкое развитие корпоративных сетей, интеграция их с информационными системами общего пользования помимо явных преимуществ порождает новые угрозы безопасности информации. Причины возникновения новых угроз характеризуются: сложностью и разнородностью используемого программного и аппаратного обеспечения корпоративных сетей; большим числом узлов сети, участвующих в электронном обмене информацией, их территориальной распределенностью и отсутствием возможности контроля всех настроек; доступностью информации корпоративных систем внешним пользователям (клиентам, партнерам и пр.) из-за ее расположения на физически соединенных носителях.

Применение описанных выше средств защиты информации, а также встроенных в операционные системы механизмов защиты информации не позволяет в полной мере ликвидировать эти угрозы. Наличие постоянных или временных физических соединений является важнейшим фактором, который влияет на повышение уязвимостей корпоративных систем из-за брешей в используемых защитных и программных средствах и утечки информации вследствие ошибочных или неграмотных действий персонала.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся: средства анализа защищенности операционных систем и сетевых сервисов; средства обнаружения опасных информационных воздействий (атак) в сетях [3].

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок и проверка наличия уязвимостей системных и прикладных служб.

Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

К числу средств анализа данного класса относится программное средство администратора ОС Solaris ASET (Automated Security Tool), которое входит в состав ОС Solaris, пакет программ COPS (Computer Oracle and Password System) для администраторов Unix-систем, и система System Scanner (SS) фирмы Internet Security System Inc. для анализа и управления защищенностью операционных систем Unix и Windows NT/ 95/98.

Использование в сетях Internet/Intranet протоколов TCP/IP, которые характеризуются наличием в них неустранимых уязвимостей, привело к появлению в последнее время новых разновидностей информационных воздействий на сетевые сервисы и представляющих реальную угрозу защищенности информации. Средства анализа защищенности сетевых сервисов применяются для оценки защищенности компьютерных сетей по отношению к внутренним и внешним атакам.

По результатам анализа защищенности сетевых сервисов средствами генерируются отчеты, включающие в себя список обнаруженных уязвимостей, описание возможных угроз и рекомендации по их устранению.

Поиск уязвимостей основывается на использовании базы данных, которая содержит широко известные уязвимости сетевых сервисных программ и может обновляться путем добавления новых уязвимостей.

К числу средств анализа данного класса относится программа SATAN (автор В. Венема), Netprobe фирмы Qualix Group и Internet Scanner фирмы Internet Security System Inc.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирования в случаях нападения на узлы корпоративной сети.

Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети [3].

Существуют определенные правила, которых целесообразно придерживаться при организации защиты информации: создание и эксплуатация систем защиты информации является сложным и ответственным процессом. Не доверяйте вопросы защиты информации дилетантам, поручи-

те их профессионалам; не старайтесь организовать абсолютно надежную защиту − такой просто не существует. Система защиты должна быть достаточной, надежной, эффективной и управляемой. Эффективность защиты информации достигается не количеством денег, потраченных на ее организацию, а способностью ее адекватно реагировать на все попытки несанкционированного доступа к информации; мероприятия по защите информации от несанкционированного доступа должны носить комплексный характер, то есть объединять разнородные меры противодействия угрозам (правовые, организационные, программно-технические); основная угроза информационной безопасности компьютерных систем исходит непосредственно от сотрудников. С учетом этого необходимо максимально ограничивать как круг сотрудников, допускаемых к конфиденциальной информации, так и круг информации, к которой они допускаются (в том числе и к информации по системе защиты). При этом каждый сотрудник должен иметь минимум полномочий по доступу к конфиденциальной информации.

Автор надется, что материал, который приведен в статье, поможет получить необходимое представление о проблеме защиты информации в компьютерных системах и успешно решать ее в повседневной деятельности.

Литература: 1. Анин Б. Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2006. – С. 12 – 78. 2. Васенин В. А. Информационная безопасность и компьютерный терроризм. Сборник "Научные и методологические проблемы информационной безопасности" / Под ред. В. П. Щерстюка. – М.: МЦНМО, 2004. – С. 34 – 68. 3. Лукацкий А. Обнаружение атак. – СПб.: БХВ-Петербург, 2007. – С. 23 – 36. 4. Франклин Куртис. Защита по правилам // Computerworld. – 2004. – С. 4 – 33. 5. Коновалов Б. Аутсорсинг — та область, где не хватает "критической массы" спроса и предложения // CNews Analytics. – 2006. – С. 107.

Евсеев С. П.

Чевардин В. Е.

Радковский С. А.

УДК 336.717:004.78

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ АУТЕНТИЧНОСТИ БАНКОВСКИХ ДАННЫХ ВО ВНУТРИПЛАТЕЖНЫХ СИСТЕМАХ КОММЕРЧЕСКОГО БАНКА

Банковская деятельность всегда связана с риском, возможной утечкой конфиденциальной информации, наличием внутренних и внешних угроз. Слабость системы экономической и финансовой безопасности, отсутствие конструктивных методов защиты банковской деятельности предопределяет её неустойчивость. На сегодняшний день научно обоснованной концепции и механизмов обеспечения финансовой безопасности банковской деятельности пока не сложилось.

Реализованные механизмы обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка отвечают требованиям к стойкости и вычислительной сложности криптопреобразований лишь на определенное время. С повышением вычислительной мощности современных супер ЭВМ (2006 г. -> 5 PFlops, 2007 г. -> 7PFlops) проблема обеспечения стойкой криптографической защиты возникает снова. Так рождаются новые, более сильные криптографические стандарты: DES->TDES->AES(256-бит), Serpent (256-бит), Twofish (256-бит), MD-4->MD-5, SHA->SHA-1->SHA-2.

Известным приемом в построении современных механизмов аутентификации является использование стойких криптопримитивов, например схемы UMAC, TTMAC, HMAC и др. Данный подход позволил свести стойкость схем аутентификации к стойкости используемого алгоритма (DES, TDES, AES и др.), что также не решило возникшей проблемы. Следовательно, современной и востребованной задачей, позволяющей решить существующие противоречия при выборе механизмов аутентификации и оценки их стойкости, является проведение анализа криптографической стойкости существующих криптопримитивов и разработка рекомендаций по обоснованию стойкости современных схем аутентификации.

Целью статьи является обоснование одного из подходов к обеспечению аутентичности банковской информации в ВПС КБ.

Особое место среди механизмов защиты является цифровая подпись (ЦП) [1], позволяющая реализовать большинство современных схем аутентификации.

Система ЦП включает две процедуры: 1) процедуру генерации подписи; 2) процедуру верификации подписи. В процедуре генерации подписи используется секретный ключ отправителя сообщения, в процедуре верификации подписи − открытый ключ отправителя. Секретный ключ хранится абонентом в тайне и используется им для формирования ЦП. Открытый ключ известен всем пользователям сети [2; 3].

При формировании ЦП отправитель вычисляет хэш-функцию h(M) подписываемого текста M, предназначенную для сжатия и перемешивания подписываемого документа M до нескольких десятков или сотен бит (фиксированной длины). Вычисленное значение хэш-функции h(M) представляет собой один короткий блок информации m (образ), характеризующий весь текст M в целом. Затем число m шифруется на личном ключе отправителя. Получаемая при этом пара чисел (необязательно) представляет собой ЦП для данного текста M (рис. 1).

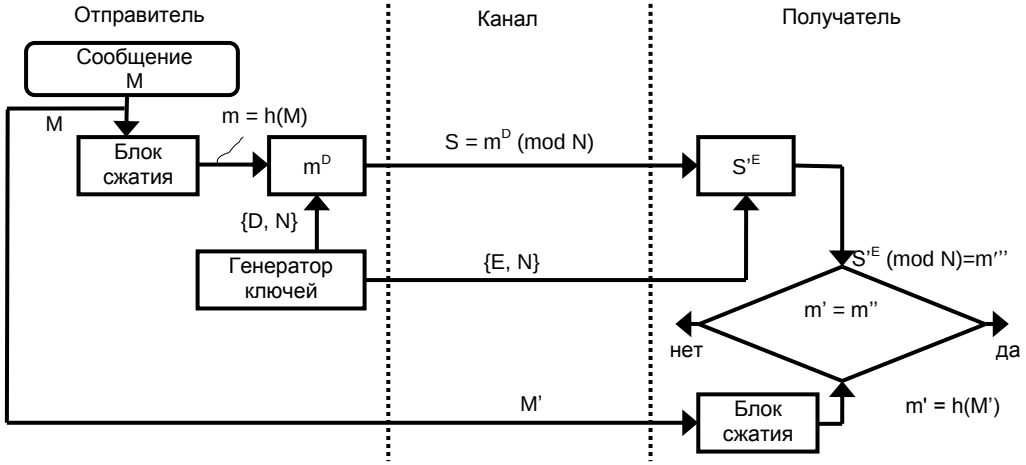


Рис. 1. **Схема формирования и верификации ЦП методом RSA**

При верификации ЦП получатель сообщения снова вычисляет хэш-функцию m' = h(M') принятого по каналу исходного текста M (возможно измененного), после чего при помощи открытого ключа E отправителя проверяет, соответствует ли полученная подпись вычисленному значению хэш-функции m' = m'' [1; 2].

Достаточно эффективным механизмом для обеспечения аутентичности сообщений является однонаправленные хэш-функции. Часть из них строится на основе симметричного блочного алгоритма шифрования в режиме CBC или CPB, с помощью фиксированного ключа и некоторого вектора инициализации IV. Последний блок шифртекста и есть хэш-значения сообщения M. При таком подходе не всегда возможно построить безопасную однонаправленную хэш-функцию, но всегда можно получить код аутентификации сообщения MAC (Message Authentication Code). Основным преимуществом этого механизма в сравнении с ЭЦП является более простой алгоритм генерации и верификации, что позволяет обеспечивать высокое быстродействие алгоритмов аутентификации сообщений в беспроводных сетях передачи данных.

Для таких механизмов длина блока определяется длиной ключа, а длина хэш-значения совпадает с длиной блока. Четыре из наиболее распространенных схем хеширования, являющиеся безопасными при всех атаках, приведены на рис. 2.

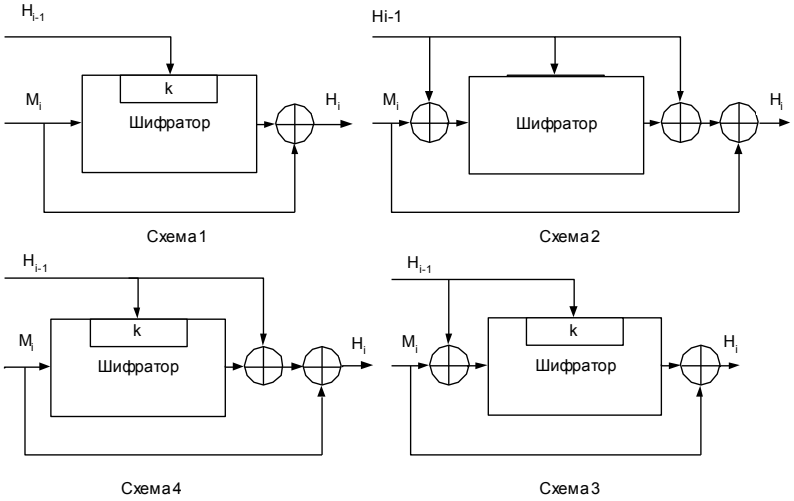


Рис. 2. **Наиболее распространенные варианты схем хеширования**

Из представленных схем (см. рис. 2) при фиксированном шифре более стойкой является схема 2, однако она является более сложной в реализации и обосновании коллизионных свойств. Последнее обусловлено результатом хеширования на предыдущем шаге h_{i-1}, который подается в качестве входа цикловой функции, в качестве ключа на i-м шаге k_{i-1} и складывается с результатом h_i. Теоретическое доказательство вероятности коллизий в таком случае является тривиальным.

Для примера рассмотрим одну из мощных современных функций хеширования ГОСТ 34.311-95. ГОСТ 34.311-95 используется в современных программных средствах "Грифон-Б" и "Грифон-Л" (ООО СНПФ "АРГУС") — обеспечивающий метод последовательного хэширования с фиксированным размером входа (функция сжатия с коэффициентом). На рис. 3 представлена обобщенная структурная схема функции хеширования по ГОСТ 34.311 – 95.

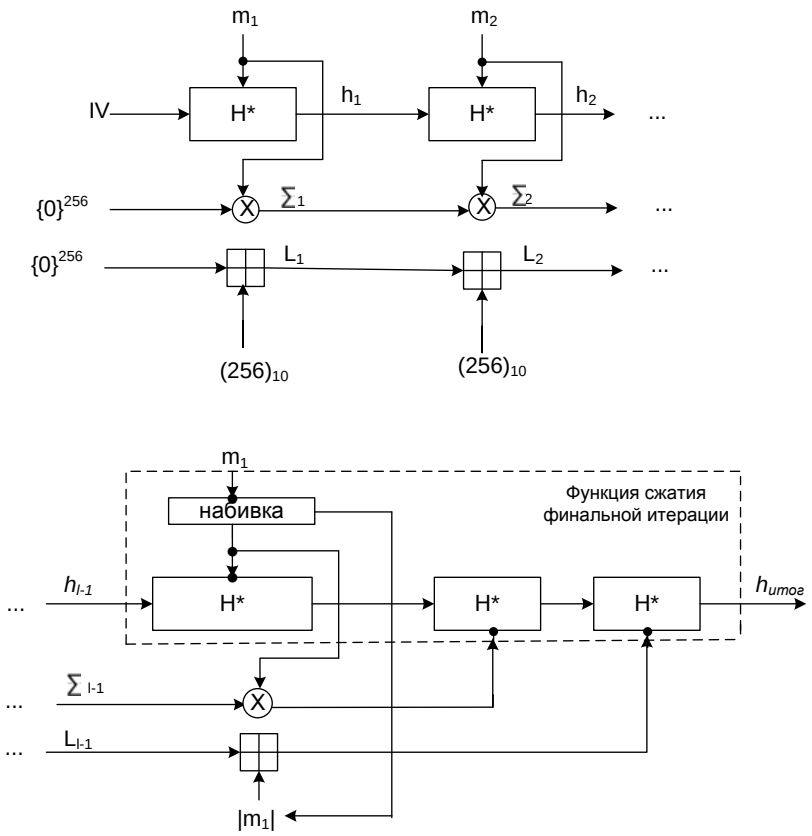


Рис. 3. **Обобщенная структурная схема функции хеширования ГОСТ 34.311 – 95**

При этом хэширование сообщения m производится в последовательности:

$$h \leftarrow IV, \quad h_i \leftarrow H(m_i, h_{i-1}) \quad \text{для } i = 1, 2, \ldots l, \quad h_{итог} \leftarrow h_l,$$

где H_i – функция сжатия, а h_i – переменная сцепления.

При необходимости последний блок заполняется до длины кратной n. В отличие от стандартных предпосылок в ГОСТ 34.311 – 95 процедура хэширования ожидает конца сообщения, а после делается "набивка".

Анализ хэш-функции по ГОСТ 34.311 – 95 позволяет сделать следующие выводы:

булева функция S-boxов линейна и ее применение неоправданно – это приводит к снижению скорости обработки данных из-за большого числа повторений перемешивающего преобразования для достижения "заданного" уровня безопасности;

шифрующее преобразование, при определенных допущениях, невозможно атаковать по частям, а, следовательно, функцию сжатия можно считать стойкой к столкновениям;

алгоритм хэширования является методом последовательного хэширования с MD – усилением (коэффициент сжатия 2);

стойкость хэш-функции в известной мере зависит от выбора блоков замен в шифрующем преобразовании, к тому же они один из параметров инициализации алгоритма хэширования;

IV в стандарте не фиксирован, а это подразумевает, что необходимо выработать правила его использования, к тому же имеется большой класс атак на псевдостолкновения при нефиксированном IV;

скорость обработки данных хэш-функцией значительно меньше, чем у аналогичных по внешним параметрам HAVAL, SHA-256, а тем более остального MD-семейства, из-за попыток ликвидировать очевидные оплошности конструирования усложнением функции сжатия;

приблизительная скорость реализации 4/5 от скорости реализации лежащего в основе алгоритма шифрования [4];

с учетом парадокса дней рождения вычислительная сложность нахождения коллизии составляет $2^{256/2}$ операций хэширования.

Это позволяет заявить о более высокой криптографической стойкости алгоритма в сравнении HAVAL, SHA-256 и потенциально высокой стойкости к коллизиям. Однако за относительно недолгое время была найдена коллизия для функций MD-5, SHA-1 подобных схеме ГОСТ 34.311 – 95. Somitra Kumar Sanadhya и Palash Sarkary получили новый метод определения коллизии на 22 шаге хеш-функции SHA-2 с вероятностью 2^{-5} и 2^{-9}. Несмотря на то, что SHA-256 имеет 64 раунда, а SHA-512 – 80 раундов, задача определения коллизии не является тривиальной. Это подтверждает в очередной раз необходимость использования отдельного класса хеширующих функций, для которых возможно теоретически обосновать верхнюю границу вероятности коллизий. Примером являются функции MMH, UMAC и др. (рис.4).

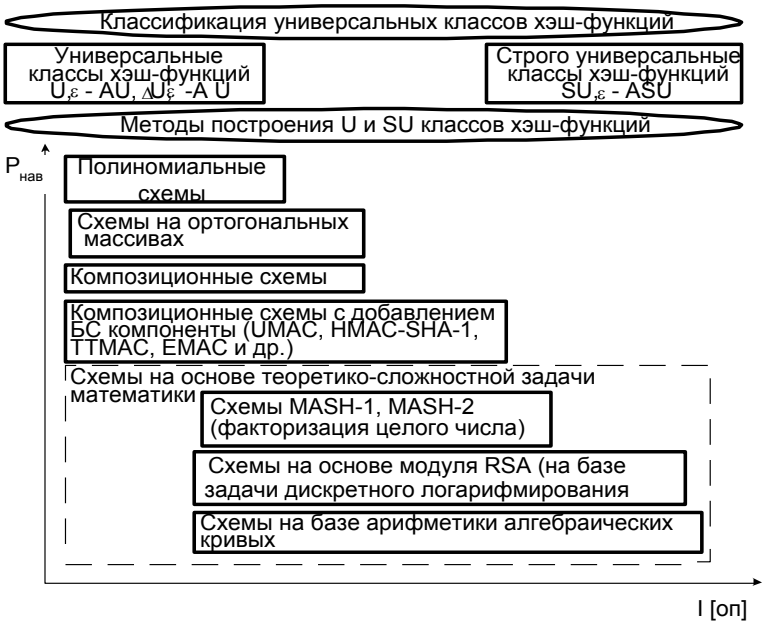


Рис. 4. **Классификация универсальных хэширующих функций**

Достоинством таких хэш-функций является сравнительно высокая скорость формирования MAC-кодов (хэш-кодов). Недостатком таких хэш-функций является слабая вычислительная стойкость. Для обеспечения требуемой ключевой стойкости необходимо по закрытым каналам передавать ключи порядка $10^3 – 10^6$ бит.

В связи с этим были предложены новые схемы хэширования: TTMAC, EMAC, HMAC и др. Основная идея в этих схемах лежит в использовании потенциально стойкого с большим периодом генератора ключевых последовательностей, шифра DES, TDES, AES. Но парадоксом в такой ситуации является сведение вычислительной стойкости схемы хэширования к стойкости используемого блочно-симметричного шифра.

Следовательно, задача обеспечения доказуемой стойкости схемы аутентификации и теоретически обоснованной верхней границы вероятности коллизий при данном подходе не решается. Решить эту задачу сегодня возможно лишь при использовании теоретико-сложностных проблем математики (дискретное логарифмирование в простом либо в группе точек эллиптической кривой) при построении цикловой функции хэширования и доказательстве ее универсальных свойств.

Таким образом, неоспоримым фактом является использование в большинстве современных ВПС КБ блочно-симметричных криптосистем. Если учесть короткое время жизни электронных транзакций в современной ВПС КБ, то заявленное значение вероятности коллизий и криптографической стойкости будет достаточно для обеспечения современных требований к схемам аутентификации. Однако, если учесть рост требований к коллизионной стойкости и доказуемой стойкости аутентификации, то очевидным является использование схем аутентификации доказуемой стойкости с теоретически обоснованной верхней границей вероятности коллизий.

Литература: 1. Столлингс В. Криптография и защита сетей: принципы и практика: Пер. с англ. – 2-е изд. – М.: Изд. дом "Вильям", 2001. — 672 с. 2. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф Шаньгин; [Под ред. В. Ф. Шаньгина. — 2-е изд., перераб. и доп. — М.: Радио и связь, 2001. – 376 с. 3. Логинов А. А. Общие принципы функционирования электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества / А. А. Логинов, Н. С. Елхимов // Конфидент. — 1995. – №4. – С. 48 – 54. 4. Шефановский Д. Б. ГОСТ 34.11 – 94. Функция хэширования. Краткий анализ. — М.: Учебн. центр "Инфозащита", 2001. – 12 с.

Чевардин В. Е.

Харыбин А. В.

Сорокин И. А.

УДК 2343.234

ОЦЕНКА СОВРЕМЕННЫХ ИНФРАСТРУКТУР ОТКРЫТЫХ КЛЮЧЕЙ

В современных телекоммуникационных системах вопрос криптографической защиты информации и обеспечения ее аутентичности и целостности достаточно важен. Это обусловлено рядом обстоятельств. Во-первых, постоянно возрастают мощности электронно-вычислительных средств, что позволяет снизить время криптоанализа используемых криптографических механизмов обеспечения безопасности информации. Во-вторых, увеличение количества услуг предоставляемых телекоммуникационными сетями, приводит к широкому использованию механизмов безопасности, в частности, электронной цифровой подписи (ЭЦП) в различных схемах аутентификации [1 – 4]. В современных компьютерных сетях механизмы аутентификации жестко привязаны к используемой инфраструктуре открытых ключей или цифровых сертификатов (ЦС) (регистрационных свидетельств) [3; 4]. В связи с этим возникает ряд проблем. Одна из них заключается в незаконной генерации ложных ЦС, примером которой являются ЦС компании VeriSign от 29.01.2001 г. и 30.01.2001 г. Вторая проблема возникла в результате конвергенции новых сетевых технологий, последствием которой являются ситуации, в которых невозможно получить ЦС либо проверить его подлинность. Это, в свою очередь, создает предпосылки для появления новых угроз безопасности информации и обуславливает актуальность исследования процессов и механизмов формирования и проверки ЦС в Украине.

Целью данной работы является рассмотрение существующих инфраструктур цифровых сертификатов, процессов аутентификации согласно ISO/IEC 11770 и ISO 11166 [3; 4] и анализ возможных подходов к построению инфраструктуры открытых ключей в Украине.

В современных автоматизированных системах, таких, как системы управления рыночными операциями, банковские, биллинговые и подобные им системы, обычно используется стандартный набор компонентов, обеспечивающих криптографическую защиту информации. В него входят: центр генерации ключевых последовательностей, центр сертификации открытых ключей (ЦСК), набор программно-аппаратного обеспечения для криптографической защиты информационных ресурсов и сетевой безопасности [2 – 4]. Особое место в такой системе занимают центры распределения открытых ключей, используемых для шифрования данных и верификации ЭЦП. Эффективность и живучесть таких центров определяет безопасность информации всей автоматизированной системы.

Основными угрозами для подобных систем являются: нарушение причастности к электронным транзакциям (получению либо отправке сообщений), нарушение их аутентичности и целостности. Для защиты от этих угроз, как правило, используют механизм ЭЦП в совокупности с процедурами сертификации открытых ключей. Так как криптоанализ современных алгоритмов электронной цифровой подписи [1; 5] для обычного пользователя сети является тривиальной задачей, то основное внимание злоумышленников сосредотачивается на способах имитации и подмены цифровых сертификатов. Возможность осуществления таких угроз зависит от отношений доверия, установленных в компьютерной системе либо сети, рост сложности которых напрямую зависит от масштаба этих систем. Следовательно, инфраструктура открытых ключей (топология сети центров сертификации) влияет на безопасность всей автоматизированной системы. Топология такой сети отображает состояние доверительных отношений между субъектами обмена информацией и влияет на процессы обеспечения аутентификации и конфиденциальности в сети [2].

В современных распределенных компьютерных сетях процессы подтверждения аутентичности открытого ключа связаны с цепочкой проверок соответствующих сертификатов в доверительных центрах сертификации (ДЦС).

Согласно Закону Украины “Про електронні документи та електронний документообіг” и “Про електронний цифровий підпис” сертификаты, которые выдаются ДЦС, оформляются в соответствии с международным стандартом X.509 [3]. В качестве алгоритмов ЭЦП используется стандарт ДСТУ 4145-2002 либо ГОСТ Р 34.310-95 и ГОСТ Р 34.311-95, которые являются действительными в Украине.

Учитывая, что каждый ЦСК может использовать свой алгоритм аутентификации, порядок этих проверок (путь) влияет на время аутентификации, степень доверия и степень риска. Для оценки существующих подходов к построению инфраструктуры открытых ключей рассмотрим каждую из них.

Инфраструктура открытых ключей (ИОК) (Public Key Infrastructure – PKI) [2; 3] – это технология, состоящая из комбинации аппаратных и программных модулей, политик и процедур, представляющая топологию сетевых связей центров сертификации, которая используется для распределения открытых ключей шифрования и цифровой подписи. ИОК является основным звеном подсистемы информационной безопасности, необходимым для надежного функционирования корпоративных информационных систем, и позволяет как внутренним, так и внешним пользователям

безопасно обмениваться информацией с помощью цепочки доверительных отношений (цепочки ЦС, связывающих личные ключи пользователей с открытыми ключами).

Современные ЦС различаются в зависимости от уровней иерархии в системе сертификации ключей.

1. С помощью ЦС 1-го уровня проверяют истинность адресов электронной почты, с помощью персонального ID, который пользователь сообщает при своей регистрации. ЦС этого уровня могут также содержать имя пользователя, а также адрес электронной почты, ID в ЦС может быть не уникальным.

2. С помощью ЦС 2-го уровня проверяют истинность имени, адреса и другой уникальной персональной информации пользователя или информации, связанной с получением разрешений (кредитов).

3. ЦС 3-го уровня используются внутри организаций, представляя собой ЦС 2-го уровня с добавлением фотографии пользователя.

Рассмотрим живучесть и безопасность известных видов ИОК.

Иерархическая инфраструктура открытых ключей

Топология связей сети ЦСК, приведенная на рис.1, позволяет получить количество проверок ЦС или цепочку сертификатов. Данная ИОК определяет простой алгоритм поиска, построения и верификации цепочек ЦС для всех взаимодействующих сторон. Для взаимодействия пользователей разных групп (ветвей ИОК) им необходимо представить цепочку сертификатов $\{ЦС_{ГЦСК}, ЦС_{ЦСК1}, ЦС_{ЦСК4}\}$.

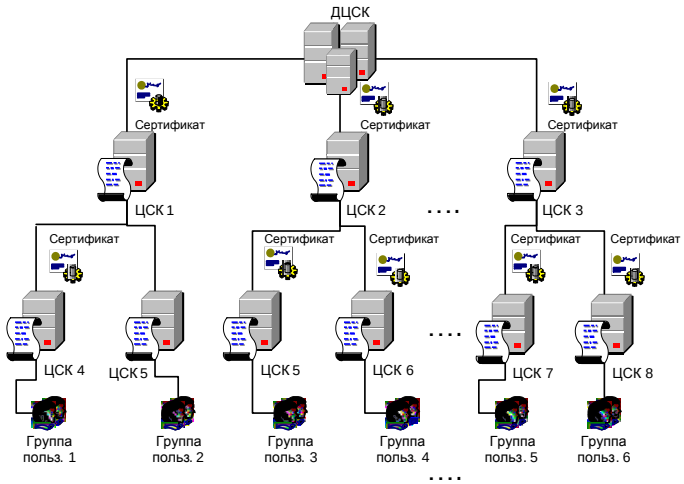


Рис. 1. **Иерархическая ИОК**

Недостатком такой ИОК является наличие только одного доверительного ЦСК (ДЦСК). Для крупных телекоммуникационных систем проверка подлинности открытого ключа будет существенно повышать время на аутентификацию объектов сети.

Сетевая инфраструктура открытых ключей

В отличии от иерархической сетевая инфраструктура (рис. 2) позволяет осуществлять непосредственную перекрестную сертификацию удостоверяющих ЦСК, пользователи которых часто взаимодействуют между собой. В итоге сокращается процесс верификации цепочек. Главной особенностью данной ИОК является повышенная живучесть. При компрометации ключа ДЦСК на определенное время (до установления нового ключа) блокируется работа не всей сети, а лишь одного домена, который обеспечивался ключами данного ДЦСК. Если же пользователи этого домена могут использовать ЦС других ДЦСК, то ИОК продолжает функционировать.

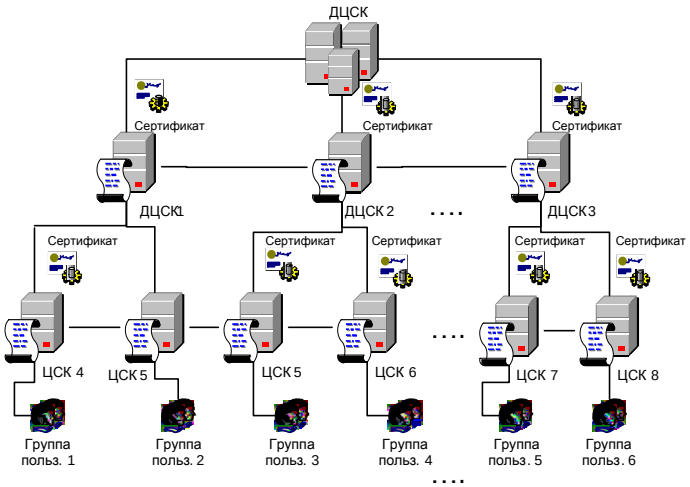


Рис. 2. **Сетевая ИОК**

Однако "узким" местом в этой иерархии является алгоритм поиска и построения цепочек ЦС. Недостатком таких алгоритмов является наличие случаев, когда не каждый пользователь сможет проверить сертификат по предоставляемой ему цепочке сертификатов. Этот случай может возникнуть при отсутствии возможности получения доступа к серверу, либо не соответствия прав пользователя политике данного ДЦСК.

Браузерная инфраструктура открытых ключей

В данной ИОК (рис. 3) каждый пользователь физически включен в несколько различных ветвей (доменов). В связи с этим для облегчения проверки сертификатов пользователей из других доменов публикуются "списки ДЦСК" Преимуществом данной модели является простота организации.

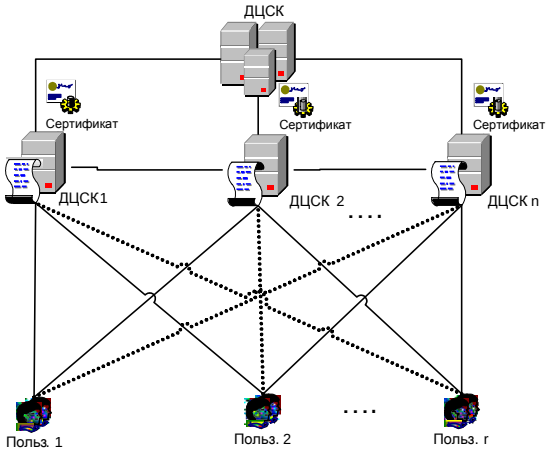


Рис. 3. **Браузерная ИОК**

Недостатком является наличие рисков при определении списков доверенных удостоверяющих центров и обеспечении защиты этих списков от несанкционированного изменения (обычно их публикация происходит через WEB-браузеры). Наиболее опасными угрозами в такой ИОК является несанкционированное изменение списков ДЦСК, их подмена либо уничтожение.

Инфраструктура открытых ключей "мост доверия"

Основная особенность такой ИОК – рост числа отношений доверия между ДЦСК. Каждая независимая ветвь ИОК перекрестно сертифицируется с мостовым удостоверяющим центром (МУЦ) соседней ветви (рис. 4). Таким образом устанавливаются равноправные отношения между различными ветвями ИОК. К достоинствам такой структуры можно отнести упрощенную процедуру проверки доверия в сравнении с предыдущими видами ИОК.

Недостатками является сложность согласования политик безопасности отдельной ветви ИОК и МУЦ, а также ЦС разных уровней. При этом в случае выполнения всех требований пользователи независимых ветвей ИОК получают возможность безопасного обмена данными. Гарантом технологической совместимости и безопасности является МУЦ.

Основные достоинства и недостатки видов ИОК представлены в таблице.

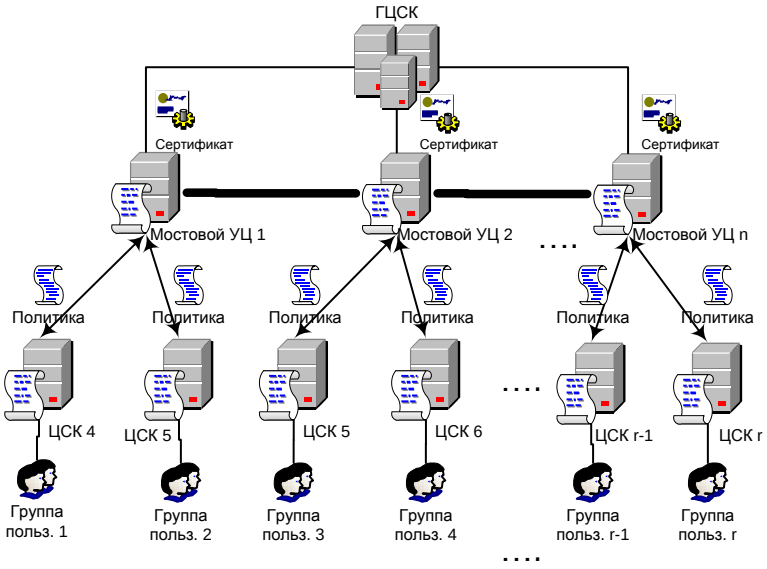


Рис. 4. **ИОК "Мост доверия"**

Таблица

Сравнительная оценка живучести и безопасности существующих видов ИОК

Вид ИОК	Достоинства	Недостатки
Иерархическая	Архитектура модели аналогична структуре ведомств (организаций); простой алгоритм поиска, построения и верификации цепочек ЦС	Для взаимодействия пользователи должны принадлежать домену одного ДЦСК; низкая живучесть ИОК; при компрометации главного ДЦСК происходит остановка работы всей ИОК
Сетевая	Повышенная гибкость ИОК; возможность перекрестной сертификации; повышенная живучесть	Усложненный алгоритм поиска, построения и верификации цепочек сертификатов; для каждого пользователя уникальные цепочки сертификатов
Браузерная	Простота и удобство организации ИОК	Наличие рисков при определении списков доверенных УЦ и обеспечении защиты этих списков от угроз целостности и подлинности
"Мост доверия"	Упрощенная процедура проверки доверия	Сложность согласования политик безопасности, правил использования сертификатов, соответствие сертификатов ИОК требованиям мостовых УЦ

Таким образом, в результате проведенной оценки живучести и безопасности современных ИОК в Украине можно сделать вывод о целесообразности построения гибридной ИОК. Гибридная ИОК позволит обеспечить повышенные требования отдельных информационных структур, осуществляющих деятельность в области IT-систем.

Каждая из составляющих частей гибридной ИОК позволит решать сугубо индивидуальные задачи снабжения открытыми ключами криптографических систем на отдельных территориях. Это позволит, во-первых, контролировать попытки несанкционированного доступа между разными участками всей инфраструктуры, а во-вторых, позволит избежать ситуаций, когда пользователь сети не может проверить подлинность информационного ресурса либо другого пользователя.

Сложностью при построении такой ИОК будет необходимость согласования политик безопасность граничных ДЦС.

Перспективным направлением дальнейших исследований является количественная оценка живучести и безопасности каждой из рассмотренных видов инфраструктур, а также разработка рекомендаций по использованию криптографических методов обеспечения безопасности информации в перспективной гибридной ИОК.

Литература: 1. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с. 2. Каплаур П. В. Постановление Совета директоров Национального банка Республики Беларусь от 19.10.2006 №281 "Об утверждении Концепции создания инфраструктуры открытых ключей" // Банківський вісник. – 2006. – №30(359). – С. 5 – 42. 3. RFC 3647. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. – Mountain View, CA: IETF, 2003. – 94 p. 4. RFC 3279. Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. – Gaithersburg, MD: IETF, 2002. – 27 p. 5. Щербаков А. Прикладная криптография / А. Щербаков, А. Домашев. – М.: Издательско-торговый дом "Русская редакция", 2003. – 416 с.

УДК 338.504

Задачин В. М.

Павленко Л. А.

ПРОБЛЕМА БЕЗПЕКИ КОМП'ЮТЕРНИХ ЕКОЛОГО-ЕКОНОМІЧНИХ СИСТЕМ, ЯКІ ПОБУДОВАНІ НА БАЗІ ГІС-ТЕХНОЛОГІЙ

Безпека будь-якої інформаційної системи (ІС) — найважливіший аспект, від якого залежить якість отримуваного продукту, а саме, інформації, яка доставляється споживачеві. З точки зору споживача інформації, як продукту, поняття "безпека" та "якість" інформації, невід'ємно пов'язані.

В еколого-економічних інформаційних системах від точності та достовірності отримуваної інформації залежить безпека та життя не тільки співробітників окремого підприємства, а й великих

прилеглих територій. Тому аналіз і впровадження технологій безпеки в комп'ютерних еколого-економічних системах є надзвичайно актуальним завданням. Особливо це стосується корпоративних інформаційних систем, де успіх інтеграції традиційних технологій обробки інформації з геоінформаційними технологіями залежить від ефективності узгодження гетерогенних потоків інформації та знань, які надходять з різноманітних джерел, за різними каналами.

Метою даної роботи є дослідження та розробка методики зниження втрат інформації в комп'ютерних еколого-економічних системах, які побудовані на базі ГІС-технологій.

Істотними відмінними рисами моделювання й аналізу навколишнього середовища, які визначають архітектуру й реалізацію інформаційної системи, є міждисциплінарність і системність аналізу, ієрархічність, наявність моделей різного рівня складності, залежність вибору підходів і моделей та сценаріїв від цілей і завдань дослідження, недостатня визначеність вхідної інформації, а також параметрів і залежностей, що входять у моделі, необхідність роботи з динамічними базами просторово-розподілених даних в оперативному режимі, у тому числі даних моніторингу і їхньому обліку при моделюванні.

Важко переоцінити необхідність використання геоінформаційних систем у еколого-економічній сфері. Інформаційна безпека еколого-економічної системи, яка розроблена та підтримується засобами геоінформаційних технологій, так само, як у будь-якій інформаційній системі залежить від таких класичних параметрів, як: точність вимірювань параметрів об'єкта спостереження, точність збору, точність передачі, точність моделювання, точність інтерпретації зібраної інформації про об'єкт дослідження. Кожен з цих параметрів необхідно досліджувати окремо, залежно від наступних факторів: природне середовище (атмосферне повітря, водне середовище, земля), клас забруднюючих речовин, погодні та сезонні умови, умови антропогенного та фонового впливу на об'єкт дослідження та багато інших.

Крім того, інформаційний дискомфорт споживача інформації у будь-якій сфері діяльності пов'язаний як з недостатньою кількістю, так і з надлишком інформації, яку він отримує, і є причиною ентропійних аномалій або "чорних інформаційних дірок" [1]. Інформаційний комфорт залежить від багатьох факторів і, в першу чергу, пов'язаний із забезпеченням "критичної маси інформації", необхідної для придушення шумів різної природи.

Особливо гостро проблема інформаційного дискомфорту проявляється як результат глобалізації бізнесу й пов'язаної із цим проблемою розподілу всіх компонентів системи управління — від функціональних до таких, що є забезпечуючими. Територіальна віддаленість підрозділів підприємств один від одного і особливо корпорацій вимагає ретельної оцінки й розробки засобів доставки й обробки інформації. Безконтрольне розширення меж предметної області для системи управління об'єктом будь-якої природи здатні викликати втрати інформаційних зв'язків з розподіленими фрагментами, або доставкою перекрученої інформації і, як наслідок, втратою засобів управління.

Відповідно до концепції дослідження інформації [2], між відправленим сигналом і одержувачем існує як би тришаровий фільтр, у кожному шарі якого відбуваються втрати інформації, обумовлені різними групами факторів. У першому шарі причиною втрат є фізичний шум, перешкоди в різних каналах зв'язку. Ця проблема вирішується наукою синтатикою. У другому шарі інформація губиться у зв'язку із семантичним шумом. У третьому шарі виконується добір інформації з урахуванням її цінності з погляду конкретного одержувача, який вирішує певні практичні завдання. Помилки в цьому доборі приводять до появи прагматичного шуму. Прагматика визначає цінність даних для конкретних споживачів з урахуванням задач, які вони вирішують.

Завдання розробників інформаційних систем можна сформулювати так: організувати збір, обробку й передачу даних таким чином, щоб втрати інформації, що вміщена в них, у всіх трьох шарах фільтра були б мінімальними. Автоматизовані інформаційні системи є діючими компонентами кіберкорпорації, виконують функції підтримки управління на всіх рівнях. Але навіть вони не рятують співробітників фірми від необхідності пошуку необхідної інформації та нагромадження й аналізу значних обсягів надлишкових даних. Вихідним посиланням при оцінці інформаційного комфорту в роботі фірми [1] є те, що добір інформації виконується з відомостей, що збирають, які не є інформацією в змісті потреб фірми, тобто не є прагматичною інформацією. Поняття: "відомості", "дані", "інформація" пропонується розрізняти в такий спосіб: із численних джерел інформації надходять відомості про об'єкт дослідження, зниження їхньої надмірності перетворює їх у вхідну інформацію, в інформаційних сховищах накопичують і зберігають дані, з яких витягають необхідну вихідну інформацію. Завдання забезпечення інформаційного комфорту полягає в одержанні максимуму інформації з відомостей, що збирають, або забезпечення "критичної маси інформації", з урахуванням безлічі обмежень.

У прикладних геоінформаційних системах досліджень та прийняття рішень у сфері екології якість інформації, як продукту споживання, залежить від точності вимірювань, передачі, точності збереження, моделювання, інтерпретації результатів аналізу.

Точність вимірювань стану навколишнього середовища залежить від якості апаратури вимірювань, фахових здібностей та наполегливості персоналу. Крім того, сучасні прикладні геоінформаційні системи орієнтовані на застосування глобальних навігаційних систем GPS та ГЛОНАС, які теж не гарантують безперечної якості доставки інформації. Завоювання ними популярності серед широкого кола користувачів пояснюється наступним:

масовий вихід на ринок GPS пристроїв і програм зробили це устаткування доступним за ціною для безлічі категорій користувачів;

експлуатація цих систем навігації абсолютно безкоштовна;

GPS та ГЛОНАС навігація покриває всю територію Землі.

Основним завданням навігаційного проекту є високоточне позиціонування різних рухливих і статичних об'єктів на місцевості. Основою системи є 24 NAVSTAR (Navigation Satellite Time and

Ranging) супутника, які працюють у єдиній мережі, що перебувають на шести різних кругових орбітах, розташованих під кутом 60□один до одного, так, щоб з будь-якої точки земної поверхні були видні від чотирьох до дванадцяти таких супутників. На кожній орбіті перебуває по 4 супутника, висота орбіт приблизно дорівнює 20200 км, період обігу кожного супутника навколо землі 12 годин. В основу роботи всієї системи закладена ідея визначення координат місця розташування об'єктів на землі на основі розрахунку відстаней до групи супутників у космосі. При цьому супутники виконують роль, точно координованих точок відліку.

Приймач становить вузькоспеціалізований міні-комп'ютер, здатний не тільки визначати місце, але й обчислити швидкість руху, показати напрямок руху й розраховувати час, необхідний для досягнення конкретного пункту призначення і багато іншого. За практичну реалізацію роботи системи відповідає чипсет GPS приймача і його ПЗУ. Від чипсета GPS приймача залежить швидкість визначення координат при включенні пристрою, точність позиціонування й чутливість приймача. На сьогоднішній день існує кілька виробників чипсетів для GPS пристроїв.

Точність вимірювань залежить від ефективності роботи всіх перелічених засобів та інструментів.

Точність передачі залежить від якості мережного устаткування.

Точність збереження залежить від якості апаратного й програмного забезпечення та якості структуризації середовища збереження на основі систематизації семантики предметної області. Внаслідок того, що головною особливістю інформації в ГІС, є просторовий розподіл з прив'язкою до координат мап, то головною цінністю картографічної інформації є синтаксис карти. Тому точність картографування та збереження цих даних є одним із головних факторів забезпечення якості інформації.

Точність моделювання залежить від адекватності обраних математичних моделей та методів обчислень.

Точність інтерпретації залежить від фахових якостей особи, яка приймає рішення.

У загальному вигляді точність інформації, як продукту, який доставляється замовнику, може бути представлена як інтегральна характеристика, залежна від усіх перерахованих вище факторів наступним чином.

$$T \to F\{T_1, T_2, T_3, \ldots, T_n\},$$

де T_1 — точність вимірювань параметрів об'єкта спостереження;

T_2 — точність збору інформації;

T_3 — точність передачі;

T_4 — точність моделювання інформації;

T_5 — точність картографування;

T_6 — точність інтерпретації зібраної інформації про об'єкт дослідження.

Окрім перерахованих аспектів в ГІС-системах додаються ще й такі. В основі ГІС-систем лежить цифрова топографічна інформація (цифрові карти). Собівартість робіт за їх створенням дуже висока. Тому виникає питання про авторське право на цифрові карти. Карти, як і будь-яка інша інформація, є інтелектуальною власністю автора чи авторського колективу. Високу цінність має тематична інформація цифрових карт (наприклад, схема інженерних мереж і комунікацій та інше), яка застосовується в ГІС [3]. Очевидно, що зміст цифрових карт, котрі використовуються у воєнних цілях, також не є інформацією для загального використання. Картографічні дані, які несуть комерційну інформацію, потребують обмеження доступу до них.

Різні розробники цифрових карт використовують два основних заходи захисту інформації: за допомогою вбудованих засобів ГІС, а також програмних та апаратних рішень сторонніх виробників [4].

На цей день найбільш поширений вид програмно-апаратного захисту даних − це електронні ключі [4]. Ці засоби дозволяють захищати цифрову карту (тобто файли, з котрих вона складається) за допомогою спеціальних алгоритмів шифровки. Цей ключ в подальшому передається споживачеві. Даний метод є ефективним, але захищати свої дані таким чином можуть тільки великі компанії, що створюють та розповсюджують ГІС-дані. Ці компанії можуть дозволити собі замовити виробництво електронних ключів для усього обсягу даних. Для невеликих компаній програмний метод підходить краще, бо, купивши програму, вони можуть поширювати захищені ГІС-дані без додаткових пристроїв.

Методика зниження втрат інформації в комп'ютерних еколого-економічних системах, які побудовані на базі ГІС-технологій, складається з багатьох етапів:

пошук і вибір об'єктів дослідження, які містять максимум інформації при моделюванні стану навколишнього середовища — інформативних джерел, що знижує надмірність відомостей і наближує їх до прагматичної інформації. При цьому фіксуються: період відновлення інформації, яка надходить від кожного джерела (якщо така інформація є). В цьому випадку пропонується використовувати моделі, засновані на нечітких множинах [5];

структуризація середовища збереження даних на основі систематизації семантики предметної області [6]. Оптимальне збереження даних забезпечується ретельною розробкою моделі збереження як картографічних, так і атрибутивних даних та розміщенням їх на серверах баз даних;

викривлення інформації на мапах, які надаються споживачам. Даний метод захисту засновано на ідеї зберігання картографічних даних у викривленому вигляді, які заносяться в цифрову карту так, щоб на перший погляд візуально зміни в карті були б непомітними. Для нелегальних користувачів координати об'єктів дослідження на карті не повинні відповідати дійсності та не є корисними для використання. Легальні користувачі отримають повноцінну інформацію;

роздільне збереження цінної інформації на різних серверах. Наприклад, структура графа інженерної мережі (газопроводи, тепломережі і таке інше) та цифрова інформація для графічного її відображення зберігаються в різних місцях, тобто втрата однієї частини інформації не призводить до втрати всієї інформації в цілому. Злочинність у результаті отримає дані, що не є придатними для застосування;

оптимізація роботи кінцевих користувачів інформаційної системи в мережі з інформативними джерелами на підставі розподілу інформаційних ресурсів;

забезпечення підтримки бази даних системи в актуальному стані з ураховуванням факта старіння інформації;

обробка інформації за короткий час в оперативному режимі;

незмінними та загальними вимогами до комп'ютерних еколого-економічних інформаційних систем, які побудовані на базі ГІС-технологій, є оптимальний вибір апаратних і програмних засобів реалізації та підтримки системи та використання традиційних апаратних та програмних засобів захисту інформації.

Пропоновані підходи та методика зниження втрат інформації в комп'ютерних еколого-економічних системах, які побудовані на базі ГІС-технологій, є досить загальними та не є універсальними, але можуть бути корисними при розробці комп'ютерних еколого-економічних систем на базі ГІС-технологій.

Література: 1. Павленко Л. А. Моделі забезпечення інформаційного комфорту роботи фірми системи підтримки прийняття рішень інформаційного менеджменту // Управління розвитком. – №3. – 2005 – С. 51 – 52. 2. Економічна інформація. Методологічні проблеми. — М.: Статистика, 1974. — 240 с. 3. Хаксхольд В. Введение в городские геоинформационные системым / Пер. с англ. – М.: Русское изд-во АГИТ, 1996. – 325 с. 4. Галатенко В. А. Стандарты информационной безопасности: курс лекций. – М.: Интернет-университет информационных технологий, 2004. – 326 с. 5. Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982. — 432 с. 6. Корнеев В. В. Базы данных. Интеллектуальная обработка информации / В. В. Корнеев, А. Ф. Гареев, С. В. Васюти, В. В. Райх. — М.: Нолидж, 2000. — 352 с.

Гросфельд Ю. А.

Комарова А. Б.

Мисюра А. А.

УДК 004.056.53

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПАКЕТНЫХ СНИФФЕРОВ

Во многих Интернет-программах для идентификации пользователя выступает его имя, а для аутентификации − пароль. Часто эти данные передаются в открытом виде или используются слабые алгоритмы аутентификации, которые основываются на неустойчивых алгоритмах шифрования. Одним из способов несанкционированного получения данной информации является анализ сетевого трафика или перехват, который производится с помощью специальной программы-анализатора пакетов (сниффера). Она перехватывает все пакеты, которые передаются в сегменте сети, и выделяет из них идентификатор пользователя и его пароль [1].

Сложность обнаружения сниффферов обусловлена тем, что данная атака по характеру действия на распределённую вычислительную систему относится к пассивному типу, то есть ничего не отсылает и не вносит изменения в хранимую информацию. Соответственно, обнаружить местонахождение сниффера можно только по признаку, что сетевая карта на данном компьютере переведена в режим прослушивания или так называемый безупорядоченный режим (promiscuous mode). По умолчанию сетевые адаптеры отсеивают пакеты с неподходящим MAC-адресом, но поддерживают данный режим (согласно спецификации PC99). А программа-сниффер перехватывает все передаваемые по сети пакеты независимо от того, совпадает заголовок пакета с MAC-адресом машины, на которой запущен сниффер, или нет [2].

Для перевода сетевого адаптера в режим прослушивания необходим специальный драйвер. Чаще всего используются следующие [3]:

драйвер от Microsoft − находится в Driver Development Kit (DDK); большинство снифферов операционной системы (ОС) Windows используют именно его;

WinPCap − специализированный драйвер, написанный в Политехническом институте Турина; используется, например, такими программами, как: Cain, EtherSnoop, NMAP;

LIBNET − драйвер, портованый с *nix; обычно используется такими же портованными программами.

Так как каждый такой драйвер определённой ОС имеет свои особенности работы в безупорядоченном режиме, следовательно, необходимым становится выбор наиболее подходящего и эффективного метода обнаружения сниффера.

Для обнаружения сниффера имеют место следующие методы [4].

Метод ICMP. Простейший из методов, в котором используется icmp-запрос (так называемый пинг). При отправке таких запросов первым делом производится сверка MAC-адресов в заголовке пакета. Если он совпадает с адресом компьютера-получателя, тогда пакет будет получен из сети и обработан. При этом на подозрительный компьютер (его IP адрес нам известен) отправляется пакет с неправильным MAC, но содержащий внутри вполне корректный IP-пакет. Компьютер, работающий в обычном режиме, на icmp-запрос с такими параметрами отвечать не будет. Компьютер с запущенным сниффером перехватит этот пакет, обработает его (благодаря корректному ядру) и мы получим icmp-ответ. Это будет главным свидетельством наличия перехватывающей программы на данном компьютере.

Метод ARP. При отправке ARP-запроса с широковещательным адресом (FF-FF-FF-FF-FF-FF) ответ будет получен от всех компьютеров в локальной сети. Если сетевая карта находится в прослушивающем режиме, то будет производиться проверка только первого октета MAC-адреса. В том случае, если он будет равен FF, пакет уже считается широковещательным. То есть необходимо отправить пакет с MAC-адресом FF-00-00-00-00-00, содержащий внутри корректный icmp-пакет (IP-адрес совпадает с адресом получателя). Обычный компьютер проигнорирует подобный пакет, а компьютер с запущенным сниффером перехватит и обработает его. Получение ответа будет свидетельствовать о наличии promiscuous mode.

Метод DNS. Современные снифферы обычно совершают обратные запросы на получение DNS по IP-адресу. В этом заключается обычный интерес, какой же ресурс скрывается за данным IP-адресом, так как IP-адреса безлики, а DNS могут хотя бы приблизительно сообщить о том, чем же является данный компьютер, сервером или простой рабочей станцией. В этом случае выполняется операция резолва IP-адреса − определение доменного имени по этому адресу.

Метод заключается в том, что в сеть выбрасывается пакет с заранее несуществующим IP-адресом. Компьютер с включенным сниффером перехватывает пакет и отправляет Resolve DNS запрос с данным IP-адресом. На сервере устанавливается специальный детектор, работающий на принципе аудита событий. Он позволит отследить все резолв-запросы, в том числе и запрос на данный несуществующий IP-адрес. Компьютер, с которого был послан запрос и будет компьютером с запущенным прослушивателем.

Особенностью данного метода является тот факт, что обычные хакерские подслушивающие программы резолят IP-адреса как только они появляются, в то время, как коммерческие снифферы откладывают это действие на период просмотра раскодированного протокола, что и надо учитывать при установке детектора.

Метод ловушки. Основан на человеческом факторе. За каждым подслушивающим устройством, будь то программа или аппаратный жучок, всегда стоит человек. И на человеческом любопытстве легко сыграть. При этом в сеть запускается пакет с именем пользователя (юзернеймом, логином) и паролем для подключения к серверу аутентификации. Данные передаются в незашифрованном виде. Обычно на какой-либо машине в сети настраивается сервис, и в сеть передаются данные о каком-либо вымышленном пользователе, не имеющем действительных привилегий. Сниффер перехватывает пакет и сохраняет данные. Человек, обнаруживший столь интересную информацию, наверняка попробует подключиться к серверу аутентификации. На сервере устанавливается специальный детектор, который регистрирует, что кто-то пытался получить доступ к серверу, используя уже известные нам логин и пароль. По IP-адресу легко определяется машина, с которой это пытались сделать. Соответственно, мы вычисляем сниффер и того, кто за этим стоит.

Метод исходящего маршрута. Создается пакет для пингования, но при этом в его заголовке указывается отдельный маршрут. Таким образом, пакет будет передаваться компьютеру А через компьютер Б. В компьютере Б отключается маршрутизация, то есть он не сможет перенаправлять данный пакет. Тогда при получении ответа можно сделать вывод о том, что пакет был перехвачен непосредственно из сети и обработан. Можно не отключать маршрутизацию на выбранном компьютере, а пронаблюдать факт перехвата пакета с помощью данных в поле TTL. Поле TTL показывает через сколько маршрутизаторов прошел пакет, и было создано специально для того, чтобы не нашедший своего адресата пакет был удален. Таким образом, направляя пакет через маршрутизатор, поле TTL будет уменьшено на единицу. Это будет свидетельствовать о том, что пакет был получен обычным образом и обычным образом обработан. В том случае, если же ответ на пакет пингования приходит, и значение поля TTL осталось без изменения, то пакет был перехвачен непосредственно из сети. То есть на проверяемом компьютере установлен сниффер.

Метод хоста. Это метод для определения сниффера на данном локальном компьютере. Проверка осуществляется следующим образом. Вводится в командной строке: # if config −a. Если в результате будет получена строчка, содержащая флаг PROMISC, то соответственно сетевая карта на данном локальном компьютере переведена в безупорядоченный режим, что свидетельствует о наличии подслушивающего устройства.

Метод сетевой латентности. Заключается в том, что компьютер с запущенным сниффером затрачивает какое-то время на обработку каждого пакета, передаваемого по сети, независимо от того, кому этот пакет предназначен. Соответственно, воспользовавшись этим, можно высчитать время отклика для каждого компьютера. Этот метод довольно громоздкий, но демонстрирует наглядные результаты. Суть в том, что в сеть запускается шторм пакетов, не принадлежащих ни одному компьютеру, с несуществующим MAC-адресом. Все машины в сети будут игнорировать их и время отклика будет таким же, как при отправке единичного пакета. Компьютер с включенным сниффером примет все пакеты и будет их обрабатывать. Время отклика существенно увеличится. Простое пингование всех машин в сети позволит нам обнаружить компьютер с запущенным сниффером.

Результаты работоспособности рассмотренных методов для различных ОС приведены в таблице.

Таблица

Работоспособность методов для различных ОС

	Метод ICMP	Метод ARP	Метод DNS	Метод ловушки	Метод исходящего маршрута	Метод хоста	Метод сетевой латентности
Windows	работает	работает	не работает	работает	не работает	не работает	работает
Linux	работает	не работает	работает	работает	работает	работает	работает

Таким образом, проведя анализ всех вышеперечисленных методов, можно установить наиболее подходящий по временным затратам и работоспособности. К сожалению, невозможно получить полной гарантии, что сниффер будет обнаружен в ста случаях из ста. Необходимо учитывать локальные особенности построения сети и организации рабочей зоны пользователей. Сейчас доступно большое число программ, позволяющих обнаружить сниффер в сети. Они могут работать как под Windows, так и под Linux на основе методов ICMP, ARP, DNS, сетевой латентности. Но наиболее эффективным обнаружение подслушивающего режима будет в том случае, если в качестве ОС будет установлен Linux.

Необходимо заметить, что сниффер является мощным инструментом в руках злоумышленников, так как он позволяет собрать необходимую информацию для осуществления атаки и таким образом может быть нанесен ощутимый ущерб безопасности сети как моральный, так и материальный. Таким образом, в общем случае снифферы нарушают конфиденциальность передаваемых и хранимых данных. Перехваченные пароли могут дать возможность получить доступ к защищаемым сегментам сети. Обычно пользователь использует один и тот же пароль для всех видов сервисов, и пароли доступа к не столь важным ресурсам нередко передаются по сети в незашифрованном виде. Это еще один фактор риска.

Лучший способ противодействия снифферам − это предотвратить какую-либо возможность для хакеров или просто любопытных устанавливать подобные программы и перехватывать информацию, передаваемую по сети в открытом незашифрованном виде. Соответственно, в ход идут организационные и криптографические методы. Дешифровка данных занимает определенный объем времени, и при стойком алгоритме кодирования нет возможности даже отсортировать пакеты, что делает работу снифферa практически бесполезной. Один из самых надежных, но недешевых способов − пользоваться в сети активными интеллектуальными хабами.

Литература: 1. Медведовский И. Д. Атака на Internet / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов. – 3-е изд. – М.: ДМК, 2000. – 336 с. 2. Мак-Клар С. Секреты хакеров. Безопасность сетей – готовые решения / С. Мак-Клар, Д. Скембрей, Д. Курц. – 4-е изд. — М.: Вильямс, 2004. – 656 с. 3. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин – М.: ДМК Пресс, 2004. – 616 с. 4. http://void. ru/content/1131

Купрейчик И. В.

УДК 336.717:004.78

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Информация играет все более важную роль в международном бизнесе и как ресурс, и как товар. За последние тридцать лет резко возрос объем доступной фирмам информации, а с внедрением новых коммуникационных технологий скорость доступа к информации увеличилась во много раз. Однако этот рост не всегда сопровождался соответствующим улучшением качества информации.

Существует множество видов и источников бизнес-информации. Основное разграничение заключается в том, из какого источника поступила информация: первичного (информация, собранная фирмой при непосредственном исследовании или взятая из отчетов об исследованиях) или вторичного (уже кем-то собранная информация, которую предстоит проанализировать). Соответствующее, связанное с этим различие состоит в том, является ли эта информация общедоступной или доступ к ней ограничен.

Все бизнес-процессы в определенной степени зависят от информации, которая необходима для снижения риска при принятии решений и разработке стратегии. Управление информацией является основной функцией управляющих в большинстве фирм, особенно в крупных компаниях и транснациональных корпорациях. Управление информацией определяет как получение своевременной, точной и необходимой информации и передачу ее работникам всех уровней. Управление, таким образом, включает сбор, интерпретацию и хранение информации в логической системе. Системы управления информацией, построенные, как правило, на базе какой-либо компьютерной программы, помогают привести информацию в более стройную систему, ускорить процесс доступа к ней и увеличить скорость передачи данных. Несмотря на это, надо знать, что от этих систем не будет толку, если компания вначале не определит, какие именно виды информации она хочет получать, а также не обозначит приоритетные направления ее использования.

Информация, равно как товары и ресурсы, превратилась в "стратегический ресурс", от которого зависит конкурентоспособность всех фирм". В действительности информация всегда была необходима для эффективного управления, но революция, произошедшая в коммуникационных системах, увеличила объем доступной информации и сделала процесс управления информацией более сложным и важным для фирмы.

Такое разделение между статической природой информации и свойством потенциальной активности знания было сформулировано Д. Хейдом (Hade): "Информация подчинена мыслям людей, а знание — это сила и свобода поступать в соответствии со своими взглядами". Несмотря на свою иллюстративность, эта точка зрения до некоторой степени экстремальна [1]. Информация является необходимым структурным элементом знания; знание можно получить интуитивно, но, по крайней мере в западных странах, обсуждается и анализируется именно то знание, которое получено путем восприятия и анализа информации.

При поиске источников информации особое внимание нужно уделять таким вопросам, как стоимость и конкретность получаемой информации, надежность и гарантии достоверности информации. К сожалению, имеется прямая зависимость (причем обычно очень тесная) между степенью конкретности информации и стоимостью ее получения. Необходима оценка надежности информации (с заданием допустимой погрешности); она должна включать источник, срок, в течение которого информация остается актуальной, и ее анализ. Репутация источника — это одно, а использование доказательств, подтверждающих ее, или "триангуляция" информации, — совсем другое.

Приведем несколько наиболее распространенных источников бизнес-информации:

правительственные учреждения;

библиотеки;

торговые ассоциации;

компании, занимающиеся частными исследованиями и информацией;

газеты и журналы;

службы бизнес-информации;

базы данных в режиме он-лайн.

Правительственные учреждения, как государственные, так и негосударственные, могут служить хорошим источником необработанных данных, особенно рыночных и макроэкономических, а также информации, касающейся регулирования. Однако часто эти данные нужно интерпретировать или анализировать. Некоторые правительственные учреждения пытаются сами сделать анализ; например, посольства Великобритании за границей предоставляют отчеты об исследованиях рынков заинтересованным компаниям, но качество их бывает разным, а иногда отчеты немногим отличаются от простого перечисления названий и адресов. В том, что касается экспортных рынков, торговые ассоциации зачастую являются более полезным источником.

Число компаний, занимающихся частными исследованиями и информацией, за последние годы выросло в несколько раз; они специализируются на сборе информации о рынках и конкурентах. Газеты и журналы представляют собой источник бесплатной, но не фильтрованной информации по широкому кругу вопросов. Службы бизнес-информации чаще всего предоставляют услуги по поиску специальной и детализированной информации на основе подписки или продажи. Обычно это коммерческие организации, но такие услуги предоставляют и академические учреждения. Примером коммерческих организаций могут быть служба кредитной информации Dun & Bradstreet или компания A. C. Nielsen, занимающаяся исследованиями рынка. В качестве примера академических учреждений можно привести Centre for Economic Forecasting при London Business School, предоставляющий макроэкономические анализы и прогнозы, и Small Business Foresight, предлагающий услуги по анализу и прогнозированию для держателей акций мелких компаний [1].

Развитие информационных технологий увеличило число и повысило уровень баз данных на CD-ROM и в режиме он-лайн, предоставляющих как количественную, в частности статистическую и подробную финансовую информацию (например, Datastream, FAME, Eurostat, NOMIS), так и качественную, такую, как информация о рынках и конкурентах, которую предоставляют службы новостей (например, Nexis, McCarthy, Reuters Business Briefing). Интернет со своей всемирной паутиной

предлагает невероятное количество информационных сайтов, а также средств обмена информацией по всему миру.

Количество источников информации растет невероятными темпами, а в процессе поиска информации фирмы опираются на использование средств поиска в режиме он-лайн, таких, как Lycos, созданный университетом Carnegie Mellon, WebCrawler или InfoSeek. Эти средства позволяют искать информацию многими способами: одни ищут по заголовкам и названиям, другие ищут сами документы, третьи еще как-нибудь. Для подписчиков количество услуг в Интернете вообще, а также в частных сетях, таких, как Microsoft Network, продолжает расти, обеспечивая доступ к конкретной, очень подробной информации.

Всегда имеется большой спрос на специфическую информацию по секторам и регионам, и он продолжает расти. Группы определенных интересов, блоки новостей и доски объявлений в Интернете позволяют выделять пучки узкоспециализированной информации и таким образом увеличивать полезность доступной информации. Обмен информацией по всему миру в режиме реального времени способствует установлению контактов и поддержанию взаимоотношений. Он быстро стал неотъемлемой частью ведения бизнеса, а неизбежный приход надежно защищенных систем электронных торгов в дальнейшем ускорит этот процесс.

Информационные технологии увеличили возможности доступа к первичным источникам информации внутри компании. Менеджерские информационные системы (MIS) и администраторские информационные системы (EIS) собирают информацию из таких источников, как отчеты о продажах, производственные отчеты, а также добывают информацию о рынках, финансах и производстве. Использование усложненных баз данных сделало возможными методы маркетинга взаимодействия, а новое программное обеспечение позволило развивать автоматизированные и даже "интеллектуальные" электронные формы. Очевидно, что качество информации зависит от качества информационной системы и профессионализма людей, отвечающих за входные данные.

Internet и информационная безопасность несовместимы по самой природе Internet. Она родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т. д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования [2].

Как известно, чем проще доступ в сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Internet – хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы файлы и программы, не говоря уже о возможности их порчи и корректировки.

Что же определяет бурный рост Internet, характеризующийся ежегодным удвоением числа пользователей? Ответ – дешевизна программного обеспечения (TCP/IP), которое в настоящее время включено в Windows, легкость и дешевизна доступа в Internet (либо с помощью IP-адреса, либо с помощью провайдера) и ко всем мировым информационным ресурсам.

Платой за пользование Internet является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию Intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров. Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

во-первых, ликвидировать физическую связь между будущей Internet (которая превратится во Всемирную информационную сеть общего пользования) и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web;

во-вторых, заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Ethernet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов;

в-третьих, перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети.

Безопасность данных является одной из главных проблем в Internet. Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Internet в деловых кругах. Одна только мысль о том, что какие-нибудь конкуренты смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора.

Каждая организация, имеющая дело с какими бы то ни было ценностями, рано или поздно сталкивается с посягательством на них. Предусмотрительные начинают планировать защиту зара-

нее, непредусмотрительные − после первого крупного "прокола". Так или иначе встает вопрос о том, что, как и от кого защищаться.

Обычно первая реакция на угрозу — стремление спрятать ценности в недоступное место и приставить к ним охрану. Это относительно несложно, если речь идет о таких ценностях, которые вам долго не понадобятся: убрали и забыли. Куда сложнее, если вам необходимо постоянно работать с ними. Каждое обращение в хранилище за вашими ценностями потребует выполнения особой процедуры, отнимет время и создаст дополнительные неудобства. Такова дилемма безопасности: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

Все это справедливо и в отношении информации. Например, база данных, содержащая конфиденциальные сведения, лишь тогда полностью защищена от посягательств, когда она находится на дисках, снятых с компьютера и убранных в охраняемое место. Как только вы установили эти диски в компьютер и начали использовать, появляется сразу несколько каналов, по которым злоумышленник, в принципе, имеет возможность получить к вашим тайнам доступ без вашего ведома. Иными словами, ваша информация либо недоступна для всех, включая и вас, либо не защищена на сто процентов.

Может показаться, что из этой ситуации нет выхода, но информационная безопасность сродни безопасности мореплавания: и то, и другое возможно лишь с учетом некоторой допустимой степени риска.

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

В банковской сфере проблема безопасности информации осложняется двумя факторами: во-первых, почти все ценности, с которыми имеет дело банк (кроме наличных денег и еще кое-чего), существуют лишь в виде той или иной информации. Во-вторых, банк не может существовать без связей с внешним миром: без клиентов, корреспондентов и т. п. При этом по внешним связям обязательно передается та самая информация, выражающая собой ценности, с которыми работает банк (либо сведения об этих ценностях и их движении, которые иногда стоят дороже самих ценностей). Извне приходят документы, по которым банк переводит деньги с одного счета на другой. Вовне банк передает распоряжения о движении средств по корреспондентским счетам, так что открытость банка задана *a priori.*

Стоит отметить, что эти соображения справедливы по отношению не только к автоматизированным системам, но и к системам, построенным на традиционном бумажном документообороте и не использующим иных связей, кроме курьерской почты. Автоматизация добавила головной боли службам безопасности, а новые тенденции развития сферы банковских услуг, целиком основанные на информационных технологиях, усугубляют проблему.

На раннем этапе автоматизации внедрение банковских систем (и вообще средств автоматизации банковской деятельности) не повышало открытость банка. Общение с внешним миром, как и прежде, шло через операционистов и курьеров, поэтому дополнительная угроза безопасности информации проистекала лишь от возможных злоупотреблений со стороны работавших в самом банке специалистов по информационным технологиям.

Положение изменилось после того, как на рынке финансовых услуг стали появляться продукты, само возникновение которых было немыслимо без информационных технологий. В первую очередь − это пластиковые карточки. Пока обслуживание по карточкам шло в режиме голосовой авторизации, открытость информационной системы банка повышалась незначительно, но затем появились банкоматы, POS-терминалы, другие устройства самообслуживания − то есть средства, принадлежащие к информационной системе банка, но расположенные вне ее и доступные посторонним для банка лицам.

Повысившаяся открытость системы потребовала специальных мер для контроля и регулирования обмена информацией: дополнительных средств идентификации и аутентификации лиц, которые запрашивают доступ к системе (PIN-код, информация о клиенте на магнитной полосе или в памяти микросхемы карточки, шифрование данных, контрольные числа и другие средства защиты карточек), средств криптозащиты информации в каналах связи и т. д.

Еще больший сдвиг баланса "защищенность − открытость" в сторону последней связан с телекоммуникациями. Системы электронных расчетов между банками защитить относительно несложно, так как субъектами электронного обмена информацией выступают сами банки. Тем не менее, там, где защите не уделялось необходимое внимание, результаты были вполне предсказуемы. Использование крайне примитивных средств защиты телекоммуникаций привело к огромным потерям.

Общая тенденция развития телекоммуникаций и массового распространения вычислительной техники привела в конце концов к тому, что на рынке банковских услуг во всем мире появились новые, чисто телекоммуникационные продукты, и, в первую очередь, системы Home Banking (отечественный аналог − "клиент − банк"). Это потребовало обеспечить клиентам круглосуточный доступ к автоматизированной банковской системе для проведения операций, причем полномочия на совершение банковских транзакций получил непосредственно клиент. Степень открытости информационной системы банка возросла почти до предела. Соответственно, требуются особые, специальные меры для того, чтобы столь же значительно не упала ее защищенность.

Наконец грянула эпоха "информационной супермагистрали": взрывообразное развитие сети Internet и связанных с нею услуг. Вместе с новыми возможностями эта сеть принесла и новые опасности. Казалось бы, какая разница, каким образом клиент связывается с банком: по коммутируемой линии, приходящей на модемный пул банковского узла связи, или по IP-протоколу через Internet? Однако в первом случае максимально возможное количество подключений ограничивается техническими характеристиками модемного пула, во втором же — возможностями Internet, которые могут быть существенно выше. Кроме того, сетевой адрес банка, в принципе, общедоступен, тогда как телефонные номера модемного пула могут сообщаться лишь заинтересованным лицам. Соответственно, открытость банка, чья информационная система связана с Internet, значительно выше, чем в первом случае.

Все это вызывает необходимость пересмотра подходов к обеспечению информационной безопасности банка. Подключаясь к Internet, следует заново провести анализ риска и составить план защиты информационной системы, а также конкретный план ликвидации последствий, возникающих в случае тех или иных нарушений конфиденциальности, сохранности и доступности информации.

На первый взгляд, для нашей страны проблема информационной безопасности банка не столь остра: до Internet ли нам, если в большинстве банков стоят системы второго поколения, работающие в технологии "файл-сервер". К сожалению, и у нас уже зарегистрированы "компьютерные кражи". Положение осложняется двумя проблемами. Прежде всего, как показывает опыт общения с представителями банковских служб безопасности, и в руководстве, и среди персонала этих служб преобладают бывшие оперативные сотрудники органов внутренних дел или госбезопасности. Они обладают высокой квалификацией в своей области, но в большинстве своем слабо знакомы с информационными технологиями. Специалистов по информационной безопасности в нашей стране вообще крайне мало, потому что массовой эта профессия становится только сейчас.

Вторая проблема связана с тем, что в очень многих банках безопасность автоматизированной банковской системы не анализируется и не обеспечивается всерьез. Более того, безопасность информации сплошь и рядом просто не может быть обеспечена в рамках имеющейся в банке автоматизированной системы и принятых правил работы с ней.

Тем не менее, наши банки уделяют информационным технологиям много внимания, и достаточно быстро усваивают новое. Необходим комплексный подход к информационной безопасности.

Информационная безопасность должна рассматриваться как составная часть общей безопасности банка, причем как важная и неотъемлемая ее часть. Разработка концепции информационной безопасности должна обязательно проходить при участии управления безопасности банка. В этой концепции следует предусматривать не только меры, связанные с информационными технологиями (криптозащиту, программные средства администрирования прав пользователей, их идентификации и аутентификации, "брандмауэры" для защиты входов − выходов сети и т. п.), но и меры административного и технического характера, включая жесткие процедуры контроля физического доступа к автоматизированной банковской системе, а также средства синхронизации и обмена данными между модулем администрирования безопасности банковской системы и системой охраны [3].

Необходимо участие сотрудников управления безопасности на этапе выбора − приобретения − разработки автоматизированной банковской системы. Это участие не должно сводиться к проверке фирмы-поставщика. Управление безопасности должно контролировать наличие надлежащих средств разграничения доступа к информации в приобретаемой системе.

Отсюда следует третья практическая рекомендация: относиться сугубо осторожно к любым сертификатам и отдавать предпочтение тем продуктам, надежность которых подтверждена успешным использованием в мировой финансовой практике. Безопасность в сети Internet.

Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet вы подвергаете риску безопасность вашей локальной сети и конфиденциальность содержащейся в ней информации. Одним из наиболее распространенных механизмов защиты является применение межсетевых экранов − брандмауэров (firewalls).

Новые технологии обеспечивают новые источники, методы доставки и обмена информацией, а также новые способы манипуляции информацией. В то время, как информационные технологии продолжают изменять характер сделок и других операций в бизнесе, предоставляют возможность связи по цепочке через электронную торговлю и способствуют сотрудничеству и созданию альянсов, становится все более важным развивать навыки управления информацией как ресурсом и товаром. Переосмысление фирмы и ее деятельности в терминах информации необходимо, чтобы использовать собственное конкурентное преимущество в целях надлежащего управления информацией.

Литература: 1. Blair D. C. The management and control of written information / D. C. Blair, M. D. Gordon // Information & Management. – 2005. – С. 239 – 246. 2. Браун С. "Мозаика" и "Всемирная паутина" для доступа к Internet: Пер. с англ. – М.: Мир: Малип: СК Пресс, 2006. – 168 с. 3. Левин В. К. Защита информации в информационно-вычислительных системах и сетях // Программирование. – 2004. – №5. – С. 5 – 16.

УДК 004.9:519.9

Грищук Р. В.

КІЛЬКІСНА ОЦІНКА РІВНЯ ЗАХИЩЕНОСТІ РАДІОЕЛЕКТРОННОГО ОБ'ЄКТА В СКЛАДНІЙ ДИНАМІЧНІЙ СИСТЕМІ ПІД ЧАС ІНФОРМАЦІЙНОГО КОНФЛІКТУ

Інтенсивність зростання кількості методів несанкціонованого доступу (МНД) до конфіденційної інформації, яка циркулює та обробляється радіоелектронним об'єктом (РЕО) у складній динамічній системі (СДС) (наприклад, персональна електронна обчислювальна машина в автоматизованій системі обробки інформації) під час інформаційного конфлікту (ІК), становить актуальну проблему з точки зору її захисту [1– 3]. Під ІК далі слід розуміти взаємодію двох сторін – методів захисту інформації (МЗІ) та МНД, цілі яких є протилежними [2 – 6].

З метою вибору оптимальної стратегії захисту інформації від МНД та оперативної локалізації або мінімізації зовнішніх (техногенні фактори) або внутрішніх (обслуговуючий персонал) загроз доцільно проводити оцінювання рівня захищеності (РЗ) РЕО, який є однією з вагомих і необхідних характеристик виконання об'єктом задач за призначенням.

Чинна нормативно-правова база з питань захисту інформації регламентує необхідність проведення процедур розрахунку кількісних або якісних оцінок РЗ, але не передбачає методів їх отримання [7]. Отже, кількісне оцінювання РЗ РЕО у СДС під час ІК є актуальною потребою сьогодення та потребує розробки нових науково обґрунтованих математичних методів.

Література за даною тематикою, як показано в роботах [1; 8], є закордонними виданнями, що носять публіцистичний характер. Реалізувати передбачені в міжнародному стандарті ISO 15408 методологічні засади оцінювання РЗ РЕО в реальних умовах експлуатації СДС досить проблематично [9]. Відомі методи кількісного оцінювання РЗ, які ґрунтуються на теоретичних моделях безпеки АДЕПТ-50 Хартсона, Бела-Лападули, MMS Лендвера і Мак-Ліна, Біба, Кларка-Вілсона та інших, характеризуються високим рівнем абстрагування та широкого практичного застосування не знайшли [8]. Запропоновані в роботі [8] показники оцінки РЗ не враховують динаміку ІК.

В Україні в рамках визначеної теми дана область досліджена недостатньо, хоча їй приділяється значна увага фахівців [3 – 6]. Запропонована у роботі [3] диференційно-логічна модель ЛМ 2х2/Т не враховує зміну ймовірнісних показників функціонування РЕО. У наукових працях [4 – 6] усунуто недоліки, притаманні моделі ЛМ 2х2/Т, але не враховано динаміку ІК. Таким чином, без урахування всіх можливих загроз і впливів на РЕО та їх випадкової природи кількісне оцінювання РЗ буде недостатньо достовірним і не відповідатиме реальному стану справ.

Метою статті є розробка методу кількісного оцінювання РЗ РЕО у СДС під час ІК, який би усував недоліки відомих методів та синтезував їх переваги.

Протягом усього періоду функціонування РЕО за призначенням $[t_0, T]$ з імовірнісним показником надійності $P_4(A_f, t)$ та відповідним імовірнісним показником захищеності $P_3(A_i, t)$, який досягається за рахунок упровадження МЗІ, об'єкту загрожують МНД, зовнішні та внутрішні загрози з відповідними ймовірностями $P_2(A_i, t)$, $P_1(A_\alpha, t)$ та $P_5(A_j, t)$, де $t_0 \geq 0$, t_0, T – моменти початку та припинення функціонування, t – поточний момент часу, $t \in [t_0, T]$. A_f, A_i, A_α, A_j – група незалежних випадкових, але сумісних подій, де $f = \overline{1, Z}$, $i = \overline{1, M}$, $\alpha = \overline{1, \text{K}}$, $j = \overline{1, N}$ (Z, M, K, N – кількість показників надійності МНД і МЗІ, зовнішніх, внутрішніх загроз відповідно). Імовірнісні показники $P_3(A_i, t)$ і $P_2(A_i, t)$ становлять повну групу подій ($P_3(A_i, t) + P_2(A_i, t) = 1$), які переводять РЕО в стан захищеності або незахищеності. Таким чином, у поточний момент t модель захищеності РЕО описується вектором стану $X[W, t]$ вигляду:

$$X[W, t] = X[P_1(\cdot), P_2(\cdot), P_3(\cdot), P_4(\cdot), P_5(\cdot), P_2(0), P_3(0), \mu, \lambda, t], \quad (1)$$

де λ, μ – інтенсивності МНД та МЗІ відповідно за початкових умов

$$\begin{aligned} &P_2(A_i, t_0 = 0) = P_{2\ поч} \quad \text{при} \quad 0 \leq P_{2\ поч} < 1 - P_{3\ поч}; \\ &P_3(A_i, t_0 = 0) = 1 - P_2(A_i, t_0 = 0) = P_{3\ поч} \quad \text{при} \quad 1 - P_{2\ поч} \leq P_{3\ поч} < 1 \end{aligned} \quad (2)$$

та обмежень

$$0 < P_1(A_\alpha, t) \le 1; \quad 0 \le P_2(A_i, t) < 1; \quad 0 < P_3(A_i, t) \le 1;$$
$$0 \le P_4(A_f, t) < 1; \quad 0 < P_5(A_j, t) \le 1. \qquad (3)$$

Виходячи з постановки задачі, поточного значення вектора стану РЕО $X[W, t]$ виду (1), початкових умов (2) та обмежень (3), оцінюванню підлягає рівень захищеності $P_3^*(A_i, t)$.

Формалізація задачі оцінювання $P_3^*(A_i, t)$ є досить складною процедурою і проводиться в декілька етапів. На першому етапі потрібно представити синтезовану структуру схеми кількісного оцінювання РЗ (рисунок).

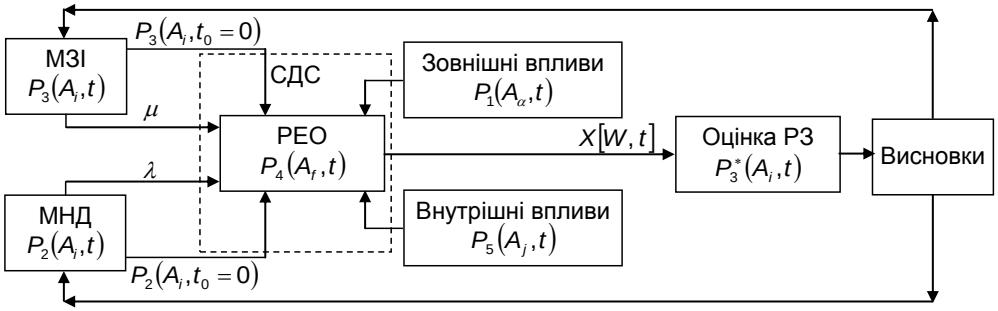


Рис. **Схема кількісного оцінювання рівня захищеності радіоелектронного об'єкта**

На другому – формалізувати поточне значення вектора стану РЕО $X[W, t]$ (1). У загальному випадку модель РЗ $X[W, t]$ під час інформаційного конфлікту набуває вигляду системи звичайних диференційних рівнянь першого порядку (Колмогорова – Чепмена) [6]. За допомогою ймовірнісного показника якісного функціонування РЕО ρ, що враховує випадковий характер $P_1(A_\alpha, t)$, $P_4(A_f, t)$ та $P_5(A_j, t)$, вона зводиться до наступного:

$$X[W, t] \equiv \begin{cases} \dfrac{dP_3(A_i, t)}{dt} = \left(-\lambda P_3(A_i, t) + \mu P_2(A_i, t)\right)\rho; \\ \dfrac{dP_2(A_i, t)}{dt} = \left(\lambda P_3(A_i, t) - \mu P_2(A_i, t)\right)\rho. \end{cases} \qquad 4)$$

Оцінка РЗ $P_3^*(A_i, t)$ може бути отримана шляхом розв'язання задачі Коші для системи (4) за початкових умов (2) та обмежень (3).

Перше рівняння системи (4), за умови $P_2(A_i, t) = 1 - P_3(A_i, t)$, зведеться до вигляду:

$$\frac{dP_3(A_i, t)}{dt} = \rho\mu - \rho(\lambda + \mu)P_3(A_i, t). \qquad 5)$$

Для розв'язування рівняння (5) щодо $P_3^*(A_i, t)$ застосовуємо пряме перетворення Лапласа:

$$L\left\{\frac{dP_3(A_i, t)}{dt}\right\} = \int_0^\infty \frac{dP_3(A_i, t)}{dt} e^{-St} dt = -P_3(A_i, S_0 = 0) + S P_3(A_i, S);$$
$$L\{\rho\mu\} = \rho\mu L\{1\} = \rho\frac{\mu}{S}; \qquad 6)$$
$$L\{-\rho(\lambda + \mu)P_3(A_i, t)\} = -\rho(\lambda + \mu)L\{P_3(A_i, t)\} = -\rho(\lambda + \mu)P_3(A_i, S).$$

З урахуванням (6) вираз (5) зведеться до наступного:

$$-P_3(A_i, S_0 = 0) + S P_3(A_i, S) = \rho\frac{\mu}{S} - \rho(\lambda + \mu)P_3(A_i, S), \qquad 7)$$

розв'язок якого щодо $P_3(A_i, S)$ матиме вигляд:

$$P_3(A_i, S) = \frac{\rho\frac{\mu}{S} + P_3(A_i, S_0 = 0)}{S + \rho(\lambda + \mu)} = P_3(A_i, S_0 = 0)\frac{1}{S + \rho(\lambda + \mu)} + \frac{\mu}{\lambda + \mu}\rho\left(\frac{1}{S} - \frac{1}{S + \rho(\lambda + \mu)}\right). \qquad (8)$$

Застосувавши до (8) зворотне перетворення Лапласа,

$$L\{f(t)\} = P_3(A_i, S_0 = 0)\frac{1}{S + \rho(\lambda + \mu)}, \text{ то } f(t) = P_3(A_i, t_0 = 0)e^{-\rho(\lambda+\mu)t}, \qquad 9)$$

$$L\{f_1(t)\} = \frac{\mu}{\lambda+\mu}\rho\left(\frac{1}{S} - \frac{1}{S+\rho(\lambda+\mu)}\right), \text{ то } f_1(t) = \frac{\mu}{\lambda+\mu}\rho\left(1-e^{-\rho(\lambda+\mu)t}\right),$$

отримаємо розв'язок задачі Коші для системи (4) при обмеженнях (3) та початкових умовах (2):

$$P_3^*(A_i,t) = P_3(A_i,t_0=0)e^{-\rho(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu}\rho\left(1-e^{-\rho(\lambda+\mu)t}\right). \quad 10)$$

З метою отримання аналітичної залежності для ймовірнісного показника якісного функціонування ρ, який ураховує надійність функціонування РЕО $P_4(A_f,t)$, зовнішні $P_1(A_\alpha,t)$ та внутрішні $P_5(A_j,t)$ загрози, на третьому етапі проводиться аналіз матриці ситуацій станів РЕО (таблиця).

Таблиця

Стратегія обмежень станів РЕО

$P_4(A_f,t)$	$P_1(A_\alpha,t)$	$P_5(A_j,t)$	ρ
0	min	min	1
0	max	max	0
0	min	max	$0<\rho\le 1$
0	max	min	$0<\rho\le 1$
max	min	min	1
max	max	max	$0<\rho\le 1$

Аналіз матриці (див. таблицю) дозволяє отримати емпіричну залежність імовірнісного показника ρ, яка набуває вигляду:

$$\rho = 1 - \left\langle \prod_{\alpha=1}^{K} P_1(A_\alpha,t) \prod_{f=1}^{Z} (1-P_4(A_f,t)) \prod_{j=1}^{N} P_5(A_j,t) \right\rangle. \quad (11)$$

Таким чином, кількісна оцінка РЗ РЕО $P_3^*(A_i,t)$ у СДС під час інформаційного конфлікту з урахуванням (11) матиме вигляд:

$$P_3^*(A_i,t) = P_3(A_i,t_0=0)\exp\left(-\left(1-\left\langle \prod_{\alpha=1}^{K} P_1(A_\alpha,t) \prod_{f=1}^{Z} (1-P_4(A_f,t)) \prod_{j=1}^{N} P_5(A_j,t) \right\rangle\right)(\lambda+\mu)t\right) +$$
$$+ \frac{\mu}{\lambda+\mu}\left(1-\left\langle \prod_{\alpha=1}^{K} P_1(A_\alpha,t) \prod_{f=1}^{Z} (1-P_4(A_f,t)) \prod_{j=1}^{N} P_5(A_j,t) \right\rangle\right) \times \quad (12)$$
$$\times\left(1-\exp\left(-\left(1-\left\langle \prod_{\alpha=1}^{K} P_1(A_\alpha,t) \prod_{f=1}^{Z} (1-P_4(A_f,t)) \prod_{j=1}^{N} P_5(A_j,t) \right\rangle\right)(\lambda+\mu)\right)t\right).$$

Таким чином, на основі системного підходу вперше отримано кількісну оцінку РЗ РЕО, яка дозволяє врахувати ймовірнісний показник якісного функціонування у СДС під час інформаційного конфлікту. У частинних випадках, при відсутності зовнішніх і внутрішніх загроз, отриманий результат (12) збігається з відомим [3]. Подальші дослідження будуть спрямовані на дослідження поведінки моделі (12) при різних початкових умовах (2).

Література: 1. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатов. – К.: Юниор, 2003. – 480 с. 2. Лістровий С. В. Теорія графів у задачах розподілу ресурсів. У 2-х кн. Кн. 2. Диференціально-ігровий підхід до моделювання систем: Підручник / С. В. Лістровий, М. І. Луханін, О. П. Мартинова, Р. В. Семчук. – Харків: ПП Вид. "Нове слово", 2007. – 144 с. 3. Ігнатов В. О. Динаміка інформаційних конфліктів в інтелектуальних системах / В. О. Ігнатов, М. М. Гузій // Проблеми інформатизації та управління. – К.: НАУ, 2005. – Вип. 15. – С. 88 – 92. 4. Козлов В. С. Количественная оценка защищённости информации / В. С. Козлов, В. А. Хорошко // Захист інформації. – 2003. – №4. – С. 67 – 73. 5. Андреев В. И. Количественная оценка защищённости технических объектов с учётом их функционирования / В. И. Андреев, В. С. Козлов, В. А. Хорошко // Захист інформації. – 2004. — №2. – С. 47 – 50. 6. Козлова К. В. Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) / К. В. Козлова, В. О. Хорошко // Захист інформації. – 2007. – №1. – С. 30 – 32. 7. ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення // http://e-signature. com. ua/?cat=13 8. Мельников В. В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с. 9. ISO 15408. The Common Criteria for Information Technology Security Evaluation // http://www. cbi-info. ru/common/

Поляков А. А.

УДК 681.3.06

ПОСТРОЕНИЕ ОБЩЕСИСТЕМНЫХ ПАРАМЕТРОВ НА ОСНОВЕ ИЗОГЕНИЙ НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ ДВА

Асимметричные криптопреобразования в группе точек эллиптических кривых на текущий момент, как де-факто, имеют стандартизированный статус в Украине. В течение последних лет был принят ряд стандартов: Национальный стандарт Украины ЭЦП [1], гармонизированные европейские стандарты схем направленного шифрования и управления ключами ДСТУ ISO [2]. В итоге сформировался полный комплекс стандартизированных криптографических алгоритмов, основанных на ЭК, который позволяет создавать криптографические системы и инфраструктуру открытых ключей, использующую одну криптографическую базу.

Как известно, криптографическая стойкость асимметричных криптосистем полностью зависит от сложности решения некоторой математической задачи. Так, криптопреобразования на ЭК относятся к классу DH-задачи. Сложность решения задач этого класса зависит от вида группы и ее параметров, то есть от возможности факторизации ЭК по подгруппам, а также от мощности группы и ряда специальных криптоаналитических атак на ЭК. Поэтому криптопреобразования на ЭК должны обладать такими параметрами, при которых обеспечивается перекрытие всех известных атак, таких, как MOV, ρ-Полларда, Полига-Хеллмана и т. д. [3; 4], а также иметь некоторый запас прочности. Все эти атаки направлены на решение только одной задачи класса DH, но существует возможность одновременного решения нескольких атак класса DH при условии, что они решаются в одной криптографической группе [5; 6]. В каждом из известных стандартов дается таблица рекомендуемых, криптографически сильных параметров ЭК. Это связано с тем, что в настоящее время в Украине отсутствует стандарт построения криптографически стойких ЭК. Сама задача построения криптографически стойких кривых является достаточно сложной как в плане затраченных вычислительных ресурсов, так и в плане реализации методов вычисления порядка ЭК. Следует отметить, что задача построения криптографически сильных общесистемных параметров (ОСП) для криптографических алгоритмов есть сложной и вычислительноемкой. При этом для обеспечения высокой криптоаналитической стойкости в таких криптографических примитивах, как протоколы управления и транспортировки ключей, требуется выработка сеансовых ключей и криптографически сильных ОСП. Это достаточно хорошо представлено в следующих протоколах [6]:

сеансовый протокол согласования ключей;

однопроходной протокол Диффи-Хэллмана;

однопроходной протокол с использованием главных ключей;

полный протокол согласования ключей.

Целью данной работы является разработка методов построения криптографически сильной эллиптической кривой на основе изогни. Для этого необходимо проанализировать как изоморфизмы, так и изогении эллиптических кривых, и рассмотреть их стойкость в каждом случае.

Теоретические сведения.

Уравнение эллиптической кривой над произвольным полем задается в обобщенной форме уравнением Вейерштрасса

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

В случае, если характеристика поля F_q отлична от 2 и 3, то уравнение Вейерштрасса может быть трансформировано к виду

$$y^2 = x^3 + ax + b$$

и является неособой кривой при условии, что дискриминант $\left(\Delta = 4a^3 + 27b^2\right) \not\equiv 0 \bmod q$.

Для полей с характеристикой два эллиптическая кривая будет неособой в следующей форме

$$y^2 + xy = x^3 + ax^2 + b,$$

при условии, что $\left(\Delta = b\right) \neq 0$ в поле F_{2^d}.

В случае ненулевого дискриминанта определен j-инвариант:

1. $j = 12^3 \dfrac{4a^3}{4a^3 + 27b^2}$ для полей с характеристикой > 3.

2. $j=\frac{1}{b}$ для полей характеристики два.

1.1. Изоморфизмы эллиптических кривых.

Изоморфизм между кривыми E_1 и E_2 задается отображением координат точек $x=\varphi(x,y)$ и $y=\phi(x,y)$, а параметры кривых связаны таким образом, что их j-инварианты равны $j_1=j_2$. В этом случае эллиптические кривые изоморфны над алгебраически замкнутым полем тогда и только тогда, когда они имеют одинаковые j-инварианты [7].

Изоморфизмы над полями характеристики, отличной от 2 и 3. Пусть эллиптические кривые E_1 и E_2 заданы над полем F_q уравнениями $y^2=x^3+a_1x+b_1$ и $y^2=x^3+a_2x+b_2$ с $j(E_1)=j(E_2)$, и существует изоморфное отображение $\phi: E_1\to E_2$. Тогда возможна замена переменных, сохраняющая j-инвариант, и отображения коэффициентов уравнения имеют вид [8]:

$$a_2=u^4a_1,\ b_2=u^6b_1,\ (x_2,y_2)=\varphi(x_1,y_1)=(u^2x_1,u^3y_1), \tag{1}$$

где $u\in\mathrm{F}_q$. Кривые E_1 и E_2 изоморфны над F_q при выполнении следующего равенства $\frac{a_1b_2}{a_2b_1}=u^2$.

Изоморфизм между эллиптическими кривыми E_1 и E_2 над расширенным полем с характеристикой 2 задается отображением φ [8]:

$$(x_2,y_2)=\varphi(x_1,y_1)=(x,y+sx),$$

а коэффициенты кривых связаны соотношениями

$$a_2=a_1+s^2+s,\ b_2=b_1, \tag{2}$$

где $s\in\mathrm{F}_{2^d}$. Кривые E_1 и E_2 изоморфны над любым расширением поля F_2, в котором уравнение $s^2+s=a_2-a_1$ относительно S имеет решение.

1.2. Изогения эллиптической кривой.

Изогения представляет собой гомоморфизм между эллиптическими кривыми $\mathrm{Hom}(E_1,E_2)$ и образуется за счет эндоморфизмов решеток C/Λ_1 и C/Λ_2, где $\Lambda_1=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$, $\Lambda_2=\mathbf{Z}\frac{n\omega_1}{\omega_2}+\mathbf{Z}$ и $n>1$. Между эллиптической кривой и решеткой существует аналитический изоморфизм. В случае $n=1$ получаем изоморфизм решеток и, соответственно, изоморфизм эллиптических кривых.

В алгебраической терминологии [8] изогения представляет собой рациональное отображение I, задающее гомоморфизм между кривыми $E_1(\mathrm{F}_q)$ и $E_2(\mathrm{F}_q)$:

$$I: E_1(\mathrm{F}_q)\to E_2(\mathrm{F}_q)$$

при условии, что выполняются следующие свойства $I(\mathrm{O})=\mathrm{O}$ и $I(E_1)\neq\{\mathrm{O}\}$. Тогда эллиптические кривые E_1 и E_2 называются изогенными.

Наибольший интерес представляет собой ядро изогении $\mathrm{Ker}\,I=\{P\in E_1: I(P)=\mathrm{O}\in E_2\}$, где P – точка на эллиптической кривой. Закон скалярного сложения точек можно рассматривать как изогению (умножение на m [8]):

$$[m]: E\to E,$$
$$[m](P)=\underbrace{P+P+\ldots+P}_{m\ раз},$$

где $m\in\mathbf{Z}$. Если $m<0$, то $[m](P)=[-m](-P)$.

Подгруппа точек m-кручения кривой $E(\mathrm{F}_q)$ является множеством точек порядка m на $E(\mathrm{F}_q)$:

$$E(\mathrm{F}_q)[m]=\{P\in E:[m]P=\mathrm{O}\}.$$

Подгруппа точек m-кручения описывает ядро изогении $[m]$.

Модулярный полином $\Phi_m(X,Y)$.

Будем использовать только арифметические свойства модулярного полинома $\Phi_m(X,Y)$, которые представлены в следующей теореме.

Теорема 1 [9]. Пусть m – положительное число.

1. $\Phi_m(X,Y) \in \mathbf{Z}[X,Y]$.

2. $\Phi_m(X,Y)$ является неприводимым, когда рассматривается как полином от одной переменной X.

3. $\Phi_m(X,Y) = \Phi_m(Y,X)$, если $m > 1$

4. Если m – неполный квадрат, тогда $\Phi_m(X,Y)$ представляет собой полином $\deg(\Phi_m) > 1$ со старшим коэффициентом, равным ± 1.

5. Если m – простое число и совпадает с характеристикой поля p, тогда $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbf{Z}[X,Y]$.

Модулярный полином имеет связь с дискриминантом D характеристического уравнения эндоморфизма Фробениуса $\pi^2 - T\pi + p = 0$, $\pi(x,y) = (x^p, y^p)$, $T = p + 1 + \#E(\mathrm{F}_p)$ [10]. Существует два случая для нечетного ℓ:

1. Если $\left(\frac{D}{\ell}\right) = 0$, то уравнение $\Phi_\ell(X,j) = 0$ имеет в поле F_p один корень или $\ell + 1$.

2. Если $\left(\frac{D}{\ell}\right) = -1$, то уравнение $\Phi_\ell(X,j) = 0$ не имеет корней.

Криптографические эллиптические кривые.

Криптографическая эллиптическая кривая определяется набором параметров: базовым полем F_q, коэффициентами a и b, порядком кривой $\#E$, кофактором h и базовой точкой $G = (x,y) \in E$ простого порядка $n = \frac{\#E}{h}$. Эти параметры называются общесистемными параметрами (ОСП).

Важным критерием криптографической стойкости эллиптической кривой является критерий стойкости эллиптической кривой к различным аналитическим атакам. К таким атакам относятся метод ρ-Полларда [3; 11] и атака изоморфизма MOV [4; 12]. Криптоаналитическая сложность метода ρ-Полларда равна $\sqrt{\pi n / 4}$ операций сложения точек и считается наименьшей. Для перекрытия атаки строятся подгруппы, порядок которых превышает 2^{192}, а для понижения криптографической сложности операций берется кофактор $0 < h \le 4$. Атака MOV позволяет осуществить переход от аддитивной эллиптической группы в мультипликативную, но большого порядка, и применить индексный алгоритм [13].

Для протоколов установления и транспортировки ключей необходимы криптографические кривые с хорошей сопротивляемостью к аналитическим атакам. Для усиления стойкости в протоколах управления ключами используют два класса ОСП: статические ОСП (static domain parameters) или сеансовые (однодневные) ОСП (ephemeral domain parameters). Статические ОСП могут использоваться либо со статическими, либо с сеансовыми ключами $\{q_s, a_s, b_s, G_s, n_s, h_s\}$. Сеансовые ОСП используются только с сеансовыми ключами $\{q_c, a_c, b_c, G_c, n_c, h_c\}$. ОСП могут распространяться в виде сертификата открытого ключа.

Пара ключей эллиптической кривой состоит из личного ключа d и открытого ключа Q. В протоколах управления ключами используются два класса ключей: пара статических ключей $\{d_s, Q_s\}$ и пара сеансовых ключей $\{d_e, Q_e\}$. Пары статических ключей являются более долговечными. Открытый ключ из пары статических ключей Q_s включается в сертификат открытого ключа. Сеансовые ключи есть краткосрочными. Они ограничиваются по длительности сообщения, количеству использований или по сеансу связи.

Построение криптографических эллиптических кривых

Как показывает практика, одной из основных задач, требующей решения, является задача построения криптографически сильных кривых, удовлетворяющих всем требованиям ОСП. Из требований к ОСП необходимо выделить два основных требования к ОСП [14 – 16]:

построение случайных кривых, коэффициенты a и b которых должны быть случайными числами;

порядок эллиптической кривой должен быть почти простым числом.

Рассмотрим задачу определения порядка эллиптической кривой. Как показывает анализ [10; 17 – 21], методы вычисления порядка эллиптической кривой накладывают свои ограничения как на порядок, так и на коэффициенты a и b эллиптической кривой. Это связано с временной (вычислительной), пространственной и алгоритмической сложностью. Поэтому можно говорить, что методы построения ОСП напрямую зависят от методов вычисления порядка эллиптической кривой. На взгляд автора, на сегодня методы построения ОСП [10; 14 – 16; 18; 19; 22] можно классифицировать по принципу построения криптографически сильной эллиптической кривой:

1. Построение ОСП на основании порядка подгруппы точек эллиптической кривой. Суть метода сводится к выбору некоторого простого числа p, удовлетворяющего требуемому уровню безопасности, и только после этого вычисляются параметры a и b соответствующей эллиптической кривой. Данный метод в основном базируется на алгоритме вычисления порядка эллиптической кривой методом "комплексного умножения". Такая методика построения ОСП используется в X9.62, X9.63, P1363 [6; 14; 16]. Применение данного алгоритма позволяет построить эллиптические кривые, удовлетворяющие всем криптографическим требованиям. Но существуют два важных ограничения:

ограничение, связанное с вычислением корня полинома классов H степени $h(D)$. При больших значениях степеней вычисление корня требует больших вычислительных затрат. В таком случае максимально допустимое значение степени, с точки зрения вычислительных затрат, равно 10000;

вычисление порядка эллиптической кривой производится заранее, и в этом случае говорить о случайности ОСП эллиптической кривой нельзя. ОСП эллиптической кривой, построенные с помощью метода "комплексного умножения", ограничены значением дискриминанта D.

2. Построение ОСП на основе изоморфных кривых. Существует возможность построения двойственной или изоморфной кривой с требуемыми криптографическими свойствами. При этом считается, что известна некоторая криптографически сильная эллиптическая кривая, удовлетворяющая всем требования ОСП, при помощи которой строятся изоморфные кривые. Этот метод используется при построении ОСП в ГОСТ 34.10-2001 [22].

3. Построение ОСП на основе случайных эллиптических кривых. К данному классу эллиптических кривых относятся кривые, порядок которых вычисляется для эллиптической кривой со случайно выбранными параметрами. Основными алгоритмами вычисления порядка эллиптической кривой являются алгоритмы Скуфа, SEA и Сато [10; 18 – 21].

Методы построения сеансовых криптографически сильных ОСП

Сеансовые ОСП должны обладать следующими требованиями:

перекрытие атаки ρ-Полларда;

перекрытие атаки MOV;

порядок базовой точки должен быть не менее 2^{192}.

Жизненный цикл сеансовых кривых ограничен маленьким промежутком времени или количеством сеансов связи. Поэтому для сеансовых ОСП требование случайности эллиптической кривой становится не строгим, а, с другой стороны, построение случайной кривой требует большого промежутка времени, что недопустимо при выполнении протоколов. Решение данной задачи без потери криптографической стойкости возможно только в направлении построения изоморфных и изогенных кривых. Такое построение эллиптических кривых основано на известной криптографической кривой и, по сути, кривые будут иметь такие же криптографические свойства, как и криптографическая кривая.

Рассмотрим построение изоморфных кривых. Переход от одной кривой к другой имеет вид (1) или (2). Сложность построения изоморфных кривых полиномиальная. Применение данного подхода приводит к появлению такой угрозы, как атака на несколько ключей с использованием одной криптографической группы. В этом случае изоморфизм $E_1 \cong E_2$ позволит выполнить переход от задачи решения дискретного логарифма на кривой E_1 к задаче решения дискретного логарифма на кривой E_2 и будет иметь вид:

$$E_1 \to E_2;$$

$$G_1 = (x_{G_1}, y_{G_1}) \to G_2 = (\alpha^4 x_{G_1}, \alpha_6 y_{G_1});$$

$$Q_1 = (x_{Q_1}, y_{Q_1}) \to Q_2 = (\alpha^4 x_{Q_1}, \alpha_2 y_{Q_1}),$$

где Q_1 и Q_2 – открытый ключ, G_1 и G_2 – базовые точки, $\alpha \in \mathrm{F}_q$ и задача дискретного логарифма кривой E_2 относительно личного ключа d имеет вид $Q_2 = d \times G_2$. Сложность атаки, направленной на одновременное вскрытие нескольких ключей, будет равна [23]:

$$I_\rho\left(\frac{2\sqrt{T}}{\sqrt{\pi}}\right),$$

где T – количество личных ключей.

Изоморфные эллиптические кривые над расширенными полями характеристики два имеют полиномиальную сложность построения и зависят только от следа коэффициента a кривой $y^2 + xy = x^3 + ax^2 + b$ при постоянном коэффициенте b. Построение таких кривых достаточно просто и оставляет возможность сведения решения задачи дискретного логарифма к одной криптографической группе.

Рассмотрим возможность использования изогений эллиптической кривой для построения сеансовых кривых.

Теорема 2 [24]. Две эллиптические кривые $E_1/\mathbf{F}_q$ и $E_2/\mathbf{F}_q$ изогены над полем $\mathbf{F}_q$, тогда и только тогда, когда их дзета-функции равны $Z\left(E_1/\mathbf{F}_q, T\right) = Z\left(E_2/\mathbf{F}_q, T\right)$.

Также известно, что дзета-функция любой эллиптической кривой E, определенной над $\mathbf{F}_q$, может быть представлена в виде рациональной функции:

$$Z\left(E/\mathbf{F}_q; T\right) = \frac{1 - aT + qT^2}{(1-T)(1-qT)},$$

где a – след Фробениуса, $a = q + 1 - \#E\left(\mathbf{F}_q\right)$.

На основании этого можно сформулировать следующее следствие.

Если существует изогения $\phi: E_1 \to E_2$ над полем $\mathbf{F}_q$, то изогенные эллиптические кривые E_1 и E_2 имеют одно и то же количество точек над полем $\mathbf{F}_q$, $\#E_1\left(\mathbf{F}_q\right) = \#E_2\left(\mathbf{F}_q\right)$.

Используя данное следствие, возможно строить неизоморфные эллиптические кривые, при этом сохраняются их криптографические свойства. Следовательно, для нахождения изогении необходимо найти некоторую подгруппу точек, которая будет являться ядром изогении. Воспользуемся результатами статей [25; 26], в которых определено существование подгрупп точек ℓ-кручения.

Для эффективного построения эллиптических кривых используем модулярный полином $\Phi(X, Y)$. Вычислив корень модулярного полинома $\Phi_\ell\left(j(E_1), \tilde{j}\right) = 0$, найдем j-инвариант $\tilde{j}$ изогенной эллиптической кривой E_2. В поле характеристики 2 коэффициенты a и b эллиптической кривой $E_2: y^2 + xy = x^3 + a_2 x + b_2$ можно вычислить по формуле:

$$b = \frac{1}{\tilde{j}}.$$

Коэффициент a_2 кривой E_2 выбирается того же следа, что и коэффициент a_1 кривой E_1, то есть

$$Tr(a_1) = Tr(a_2).$$

Данный метод построения эллиптических кривых для сеансовых ОСП с использованием известных криптографически стойких ОСП позволяет повысить безопасность. В этом случае криптоаналитику для взлома личного ключа объекта потребуется использовать две криптоаналитические системы с различными ОСП.

Для построения ОСП данным методом необходимо, чтобы эллиптическая кривая имела достаточно большой составной кофактор h. Также следует учитывать, что при изогении точки кривой, не принадлежащие ядру изогении, остаются неподвижными, а построить изогению равную порядку криптографической группы, невозможно из-за большой размерности ее порядка. В этом случае целесообразно рассматривать двойственные эллиптические кривые E', чья структура не является криптографической и содержит подгруппы небольших порядков, для которых можно строить изогении. Соответственно двойственной к E' будет кривая, чьи свойства будут криптографическими.

В поле характеристики два существует особенность относительно двойственных и обычных эллиптических кривых [25]. У обоих кривых j-инварианты равны. В этом случае нам не потребуется строить двойственную эллиптическую кривую.

Данный метод в разделе поиска подгрупп точек может быть усовершенствован, используя знания порядка криптографической эллиптической кривой, а соответственно, и дискриминанта D. Это позволит избежать вычисления корней модулярных полиномов $\Phi_\ell(X, j)$. Вычисление корней модулярного полинома потребуется одноразово только после нахождения символа Лежандра $\left(\frac{D}{\ell}\right)$, равного 0.

Таким образом, в работе предложены методы построения сеансовых ОСП в реальном масштабе времени для применения их в протоколах управления ключами. Эти методы не позволяют строить случайные эллиптические кривые, но имеют связь со случайной криптографической кривой. Такой способ построения сеансовых эллиптических кривых даст возможность не менять базового поля, а следовательно, и оптимизированную библиотеку многократной точности.

Литература: 1. ДСТУ. Національний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. – К.: Держстандарт, 2003. – 40 с. 2. ДСТУ. Національний стандарт України. Інформаційні технології. Методи захисту криптографічних перетворень, що ґрунтуються на еліптичних кривих. Ч. 3: Встановлення ключових даних (ISO/IEC 15946-3, IDT). – К.: Держстандарт, 2006. – 68 с. 3. Горбенко И. Д. Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда / И. Д. Горбенко, С. И. Збитнев, А. А. Поляков // Всеукр. межвед. науч-тех. сб. "Радиотехника". – 2001. – Вып. 119. – С. 43 – 50. 4. Shikata J. et al. Ralizing the Menezes-Okamoto-Vanstone (MOV) Reduction Efficienly for Ordinary Elliptic Curves // IEICE Trans. Fundamentals, – 2000. – Vol. E83-A(No. 4). – P. 756 – 763. 5. Silverman J. H. and J. Stapleton, Contribution to ANSI X9F1 working group. 1997 // www. ANSI. org. 6. ANSI, Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 2001. 7. Husemöller D. Elliptic curves, 2nd ed. – New York: Springer-Verlag, 2004. – 488 p. 8. Silverman J. H. The Arithmetic of Elliptic Curves. – New York: Springer-Verlag, 1986. – 416 p. 9. Cox D. A. Primes of the form x2+ny2: Fermat, class theory, and complex multiplication. – New York: JOHN WILEY & SONS, INC., 1989. – 352 p. 10. Schoof R., Counting points on elliptic curve over finite fields // Journal de Theories des Nombres de Bordeaux. – 1995. – Vol. 7. – P. 219 – 254. 11. Van Oorschot P. C. and M. J. Wiener, Parallel Collision Search with Cryptanalytic Applications // Journal of Cryptography. – 1999. – Vol. 12(No. 1) – P. 1 – 28. 12. Menezes A. J., T. Okamoto and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Transactions on Information Theory. – 1993. – Vol. 39(No. 5) – P. 1639 – 1646. 13. Бессалов А. В. Криптосистемы на эллиптических кривых / А. В. Бессалов, А. Б. Телижненко. – К.: Политехника, 2004. – 224 с. 14. ANSI, Public Key Cryptography For The Financial Services Industry // The Elliptic Curve Digital Signature Algorithm (ECDSA). 1999. 15. ISO/IEC, Information Technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signature. 2002. – 29 p. 16. IEEE, Standard Specifications for Public Key Cryptography. 1999: New York. 17. Buchmann J. and H. Baier. Efficient Construction of Cryptographically Strong Elliptic Curves. in Progress in Cryptology — INDOCRYPT 2000, First International Conference in Cryptology in India. Proceedings. 2000. Calcutta, India: Springer. 18. Schoof R. Elliptic curve over finite fields and the computation of square roots mod p. Mathematics of Computation., 1985. – Vol. 44(No. 170) – P. 483 – 494. 19. Couveignes J. M., L. Dewaghe and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research Report LIX/RR/96/03. 1996, LIX. – 17 p. 20. Skjernaa B. Satoh's algorithm in characteristic 2. Mathematics of Computation. – 2003. – Vol. 72(No. 241). – P. 477 – 487. 21. Satoh T. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. J. Ramanujan Math. Soc., 2000. – Vol. 15(No. 4). – P. 247 – 270. 22. ГОСТ. Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи. – М.: Госстандарт, 2001. 23. Kuhn F. and R. Struik. Random Walks Revisited: Extensions of Pollard's Rho Algorithm for Computing Multiple Discrete Logarithms. in Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001. Revised Papers. 2001. Toronto, Ontario, Canada: Springer. 24. Silverman J. H. A survey of the arithmetic theory of elliptic curves, in Modular forms and Fermat's last theorem. 1997, Springer-Verlag: New York. – P. 17 – 40. 25. Горбенко И. Д. Метод анализа структуры группы точек эллиптической кривой на содержание подгрупп малого порядка над расширенными полями характеристики 2 / И. Д. Горбенко, А. А. Поляков // Прикладная радиоэлектроника. – 2007. – Т. 6(№2). – С. 315 – 325. 26. Поляков А. А. Метод нахождения случайной криптографически стойкой эллиптической кривой на расширенных полях характеристики 2 // Всеукр. межвед. науч-тех. сб. "Радиотехника". – 2003. – Вып. 134. – С. 149 – 156.

УДК [004.056:351.862.4](075.8)

Живко М. О.

Босак Х. З.

ЕКОНОМІКО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Інформаційна безпека в правовому вимірі виступає як невід'ємна складова сучасної системи управління на шляху до правової держави і як суттєвий чинник формування громадянського суспільства та входить до більш широкого розуміння питань національної безпеки загалом, а з розвитком новітніх технологій ще виокремлюється напрямок комп'ютерної безпеки.

За таких умов законодавча невизначеність щодо основних параметрів інформаційної безпеки, існуючі суперечності та прогалини у правозастосовчій практиці в цій сфері ускладнюють внутрішні трансформаційні перетворення та інтеграцію України у світові цивілізаційні процеси. А тому це робить надзвичайно важливим глибокий науково-теоретичний аналіз та вдосконалення практичної діяльності щодо підвищення рівня інформаційної безпеки на сучасному етапі розвитку України.

Світові процеси глобалізації, впровадження новітніх інформаційних технологій, формування інформаційного суспільства посилюють важливість такої складової національної безпеки, як інформаційна безпека. Вже найближчим часом саме розвиток інформаційної сфери, рівень інформаційної безпеки будуть визначати: політичну та економічну роль окремих держав на світовій арені; поділ країн за інформаційною ознакою; процеси демократизації й подолання наслідків тоталітаризму в самій Україні. Українська держава включена в процес загальної інформатизації суспільства і формування єдиного світового інформаційного ринку.

Серед вітчизняних науковців, які досліджують на достатньо серйозній методологічній основі проблеми національної безпеки взагалі та її складової – інформаційної безпеки – зокрема, можна назвати таких, як: В. Горбулін, Н. Нижник, Г. Ситник, В. Білоус, О. Данільян, О. Дзьобань, М. Панов, В. Ліпкан, М. Левицька, О. Бодрук, О. Гончаренко, Є. Лисицин, Ю. Максименко, В. Желіховський, Б. Кормич, О. Юдін, В. Богуш та ін.

Мета статті полягає в розкритті сутності та проблем захисту інформації в комп'ютерних системах і вагомого фактора захищеності її в інформаційній сфері, що визначаються сукупністю збалансованих економічних та правових аспектів інформації.

Широке застосування інформаційних технологій поряд з позитивними впливами на всебічну людську діяльність спричинило появу нових загроз безпеці людства. Це пов'язано з тим, що інформація, створена, збережена й опрацьована технічними засобами, почала визначати дії більшості людей і технічних засад. Тому різко зросли можливості завдання шкоди, пов'язані з крадіжкою інформації. Адже вплив на будь-яку систему (соціальну, біологічну, технічну, комбіновану) з метою її знищення може бути реалізованим за наявності вірогідної інформації про структуру та особливості функціонування системи. Отримана інформація супротивником може використовуватися не лише для повного знищення системи, а й для незаконного заволодіння ресурсами (грошовими коштами, товарами, засобами, інтелектуальною власністю). Недаремно постулатом став вислів: "Хто володіє інформацією, той володіє світом", адже наявність інформації про бізнес-конкурентів – це запорука ефективності вашого бізнесу. Всі види інформаційних загроз прийнято розділяти на дві групи:

1) відмови й порушення працездатності програмних і технічних засобів:

порушення, які виникають внаслідок неумисного пошкодження технічних засобів (через перепади електроенергії, заводський брак тощо);

порушення фізичної та логічної цілісності збережених в оперативній і зовнішній пам'яті структур даних, що виникають через старіння чи попередню втрату працездатності їх носіїв;

порушення, які виникають у роботі оперативних засобів через їх старіння чи попереднє зношення;

порушення, які виникають через неправильне поводження з програмним забезпеченням;

порушення, які виникають внаслідок неправильної експлуатації технічних засобів;

не усунені помилки в програмних засобах, які не виявлені під час перевірок і випробувань;

порушення, які виникають внаслідок некоректного поводження з комп'ютерними ресурсами;

2) умисні загрози, попередньо заплановані правопорушниками для нанесення шкоди:

загрози, реалізації яких виконуються з постійною участю людини;

загрози, реалізація яких після розроблення правопорушником відповідних комп'ютерних програм виконується цими програмами без участі людини (запуск певних вірусів, несанкціоноване "скачування" інформації тощо).

Отже, захист інформації для бізнесу важливий як у економічному, так і в правовому ракурсі.

Національна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз. Наш акцент саме на понятті "національна безпека" ґрунтується на принциповому положенні про те, що інформаційна безпека співвідноситься з національною безпекою за схемою "частина та ціле". Причому інформаційний аспект національної безпеки виступає її невід'ємним компонентом. Отже, так само як інформаційна безпека не може існувати поза межами загальної національної безпеки, національна безпека не буде всеохоплюючою у випадку позбавлення своїх інформаційних векторів.

Важлива роль охорони інформації випливає з розуміння того, що:

охорона інформації є не тільки однією з головних складових національної безпеки держави, а й невід'ємною компонентною всіх інших її складових;

інформаційні стратегії в сучасних умовах набувають важливого значення під час реалізації різних моделей співробітництва або відіграють роль своєрідної „інформаційної зброї";

руйнування та дезорганізація інформаційної інфраструктури держави прирівнюються за наслідками до застосування зброї масового знищення.

Наявна законодавча база України з питань захисту інформації в інформаційній сфері впродовж останніх років поповнилася наступними законами: „Про інформацію" [1], „Про державну таємницю" [2], „Про захист інформації в автоматизованих системах" [3], „Про науково-технічну інформацію" [4], „Про Службу безпеки України" [5], „Про міліцію" [6] тощо. Однак наше законодавство не встигає за розвитком новітніх технологій, особливо пов'язаних з розвитком комп'ютерної техніки. Тому проблеми правового регулювання боротьби з комп'ютерною злочинністю сьогодні стоять досить гостро. Кіберзлочинці настільки вміло та професійно використовують досягнення НТП, що навіть професіонали із захисту інформації приватних та державних структур, не говорячи про правоохоронців, які не є спеціалістами з комп'ютерної техніки, з труднощами вирішують поставлені завдання.

Важливе місце серед технічних каналів витоку інформації посідають акустичні. Відомо, що для людини слух є другим за інформативністю після зору. В акустичних каналах переносником інформації (мова, шуми) виступає звук, що лежить у смузі ультра (більше 20 000 Гц), слухового й інфразвукового діапазонів. Найпоширенішим способом несанкціонованого одержання інформації приватного і комерційного характеру з акустичних каналів витоку стало прослуховування телефонних переговорів об'єкта та перехоплення комп'ютерної інформації. Яскравим прикладом радіотехнічного КВ є перехоплення комп'ютерної інформації. Для дистанційного несанкціонованого зчитування вмісту або комп'ютера є два найбільш розповсюджені способи. Перший — прийом паразитних радіовипромінювань комп'ютера. Другий спосіб, що базується на прийомі високочастотних наведень на силову мережу через блок живлення комп'ютера, вимагає безпосереднього підключення до силової мережі і наступного надзвичайно складного опрацювання прийнятої інформації.

Існують матеріально-речовинні канали витоку інформації. Особливість цього каналу спричинена специфікою джерел і носіїв інформації порівняно з іншими каналами. Джерелами та носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро- та мікрочастинки), що мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Необхідно підкреслити, що нелегальні методи збору інформації мають місце в дійсності і їх треба знати, хоча б для того, щоб захищати власні таємниці комерційного чи приватного характеру.

Не менш важливими є роботи з технічного захисту інформації (ТЗІ) в інформаційних системах і ЗОТ, які передбачають: 1) класифікацію за категоріями об'єктів електронно-обчислювальної техніки (ЕОТ); 2) включення до технічних завдань на монтаж ІС і ЗОТ розділу з ТЗІ; 3) монтаж ІС і ЗОТ відповідно до рекомендацій цього документа; 4) обстеження об'єктів ЕОТ; 5) технічний контроль об'єктів ЕОТ; 6) установлення атестованих засобів захисту; 7) технічний контроль за ефективністю вжитих заходів.

Канали поширення інформації − це засоби обміну ділової та наукової інформації між суб'єктами ділових і приватних взаємин. На підставі аналізу практики боротьби з комп'ютерними злочинами та зарубіжного кримінального законодавства слід наголосити на підвищеній суспільній небезпечності цього способу, яка зумовлюється тим, що: 1) для подолання заходів інформаційної безпеки технічного чи програмного характеру потрібні спеціальні знання, специфічні навички; 2) шкода власникові заподіюється не лише у вигляді знищення або перекручення комп'ютерної інформації, але й в істотних матеріальних витратах, що зумовлюється необхідністю відновлення чи заміни системи захисту. Це й визначає доцільність виділення несанкціонованого доступу як кваліфікуючої ознаки складу незаконного втручання, передбаченого в ч. 2 ст. 361 КК України, зазначивши: "Ті самі дії ... вчинені шляхом несанкціонованого доступу до комп'ютерної інформації".

Основним засобом заборони несанкціонованого доступу до ресурсів обчислювальних систем є підтвердження достовірності користувачів і розмежування їм доступу до інформаційних ресурсів, які включають наступні етапи: ідентифікація; встановлення достовірності; визначення повноваження для наступного контролю й розмежування доступу до комп'ютерних ресурсів; розмежування за системами (користувачів чи ресурсів); використання матриці встановлення повноваження (строки матриці − ідентифікатори користувачів, ресурси комп'ютерної системи); розмежування за рівнями таємності і категоріями − загальний доступ, для службового користування, таємний; парольні розмежування; кодування інформації.

Література: 1. Закон України "Про інформацію" від 02.10.1992 // Відомості Верховної Ради України. – 1992. – №48. – Ст. 650. 2. Закон України "Про державну таємницю" від 21.01.1994 р. У редакції Закону №1079-XIV (1079-14) від 21.09.1999 р. // Відомості Верховної Ради України. – 1994. – №16. – Ст. 93. 3. Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994 р. // Відомості Верховної Ради України. – 1994. – №31. – Ст. 286. 4. Закон України "Про науково-технічну інформацію" від 25.06.1993 р. // Відомості Верховної Ради України. – 1993. – №33. – Ст. 345. 5. Закон України "Про Службу безпеки України" від 25.03.1992 р. // Відомості Верховної Ради України. – 1992. – №27. – Ст. 382. 6. Закон України "Про міліцію" від 20 грудня 1990 р. // Відомості Верховної Ради України. – 1991. – №4. – Ст. 20. 7. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. із змінами від 8 грудня 2004 р.: Офіц. видання. – К.: Вид. дім „Ін Юре", 2006.

Заєць В. В.

Чуприн В. М.

УДК 004.056.5(045)

РОЗРАХУНОК ЕФЕКТИВНОСТІ КРИПТОСЕМАНТИЧНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Для захисту особливо важливої (в тому числі таємної) інформації у спеціалізованих прикладних системах останнім часом знайшли застосування криптосемантичні (КСМ) методи захисту [1], тому оцінка ефективності КСМ-систем викликає певний практичний інтерес. У даній роботі пропонується один із можливих варіантів розрахунку ефективності КСМ-системи захисту за умов дотримання властивостей досконало секретних систем захисту [2].

Побудуємо залежність відстані одиничності від довжини повідомлення. Отже, відстань одиничності [3] визначається наступним виразом:

$$U = \frac{H(K)}{D}, \tag{1}$$

де $H(K)$ − ентропія системи захисту інформації (СЗІ);
D − надлишковість мови.

Ентропія системи захисту інформації (СЗІ) $H(K)$ є мірою розміру простору ключів K, а саме:

$$H(K) = \log_2 K, \tag{2}$$

де K − кількість можливих ключів у СЗІ.

Надлишковість мови обчислюється за формулою:

$$D = R - r, \tag{3}$$

де R − це максимальна ентропія окремих символів мови;
r − ентропія мови.

Відповідно

$$R = \log_2 B, \tag{4}$$

де B − кількість символів алфавіту, яка визначається за формулою:

$$B = \prod_{i=1}^{s} S_i, \tag{5}$$

де s − кількість підсловників у тезаурусі вибраної табличної форми;
S_i − кількість слів (чи словосполучень) в і-му підсловнику тезаурусу.

Ентропія мови r, за допомогою якої відображається повідомлення M, визначається за наступною формулою:

$$r = \frac{H(M)}{n}, \tag{6}$$

де $H(M)$ − ентропія повідомлення,
n − довжина повідомлення.

Ентропія повідомлення вимірюється у бітах і дорівнює:

$$H(M) = \log_2 N, \tag{7}$$

де N − кількість можливих значень повідомлення.

Отже,

$$U = \frac{H(K)}{\log_2(B) - \frac{H(M)}{n}}. \tag{8}$$

Виходячи з властивостей досконало секретної системи, кількість ключів K повинна дорівнювати N − кількості повідомлень довжиною n. Таким чином, за умовою $H(K) = H(M) = \log_2 N$ можна записати наступний вираз:

$$U = \frac{log_2 N}{log_2(B) - \frac{log_2 N}{n}}. \tag{9}$$

Тепер знайдемо залежність *N* − кількість можливих значень повідомлення від *n* − довжини повідомлення. При визначені *N* слід мати на увазі те, що кожен рядок у таблиці (тобто кожна літера в повідомленні) зустрічається тільки один раз (тобто літери не повторюються). У цьому випадку максимально можлива довжина повідомлення дорівнює кількості літер в алфавіті. Отже, запишемо вираз для визначення *N* − кількості можливих значень повідомлення при різних *n*:

$$N = \prod_{n=1}^{n}\left[B-(n-1)\right]. \tag{10}$$

Таким чином, при *B* = *const* і при $H(K)=H(M)$ (умова досконало секретної системи) можна записати наступне:

$$U(n) = \frac{\log_2 \prod_{n=1}^{n}\left[B-(n-1)\right]}{\log_2(B)\ \ \frac{\log_2 \prod_{n=1}^{n}\left[B-(n-1)\right]}{n}}. \tag{11}$$

Залежність ентропії ключа *H(K)* від довжини повідомлення *n* можна записати наступним чином:

$$H(K) = \log_2 \prod_{n=1}^{n}\left[B-(n-1)\right]. \tag{12}$$

Приклад.

Нехай маємо тезаурус, що складається з чотирьох підсловників, тобто *s = 4.* Ці підсловники мають певну кількість лінгвістичних одиниць, а саме: $S_1 = 3$, $S_2 = 6$, $S_3 = 3$, $S_4 = 3$. Побудуємо графіки залежності $U = f(n)$, $H(K) = f(n)$.

Визначимо *B* за формулою:

$$B = \prod_{i=1}^{s} S_i \tag{13}$$

Отже, *B = 162* − кількість літер алфавіту, і максимальна довжина повідомлення, оскільки кожна літера в повідомленні зустрічається тільки один раз. Побудуємо графік залежності відстані одиничності від довжини повідомлення (рис. 1).

З графіка на рис. 1 видно, що навіть при максимальній довжині повідомлення *n = 162* відстань одиничності $U \approx 680$ символів. Результати розрахунків повністю підтверджують теорію Шеннона, який стверджував, що шифротексти, які значно коротші за відстань одиничності, можна дешифрувати декількома способами, причому кожен з них може бути коректним, і, таким чином, забезпечити захист повідомлення, поставивши криптоаналітика перед вибором правильного повідомлення із множини кількох можливих повідомлень.

Побудуємо графік залежності ентропії ключа *H(K)* від довжини повідомлення *n* (рис. 2) за виразом:

$$H(K) = \log_2 \prod_{n=1}^{n}\left[B-(n-1)\right]. \tag{14}$$

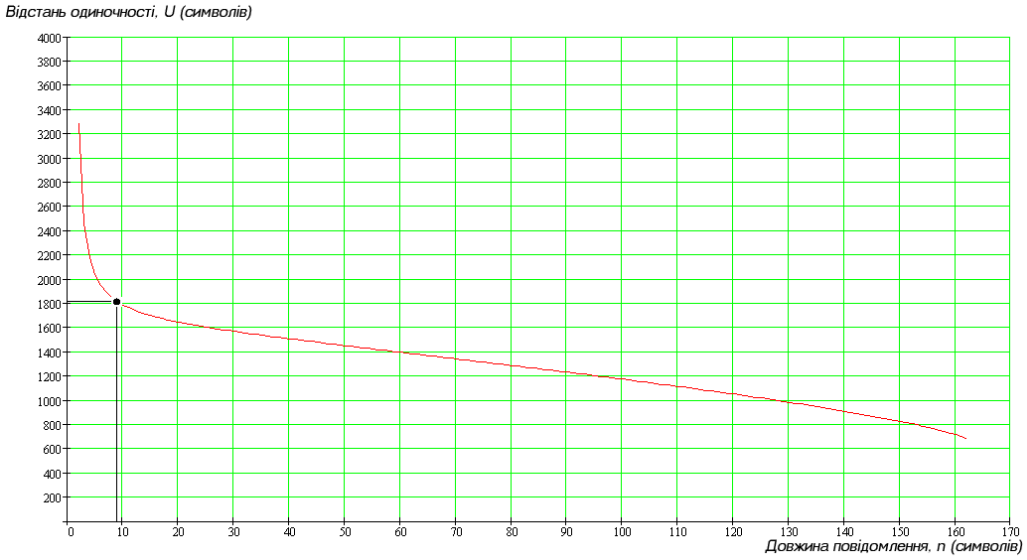


Рис. 1. **Графік залежності відстані одиничності *U* від довжини повідомлення *n***

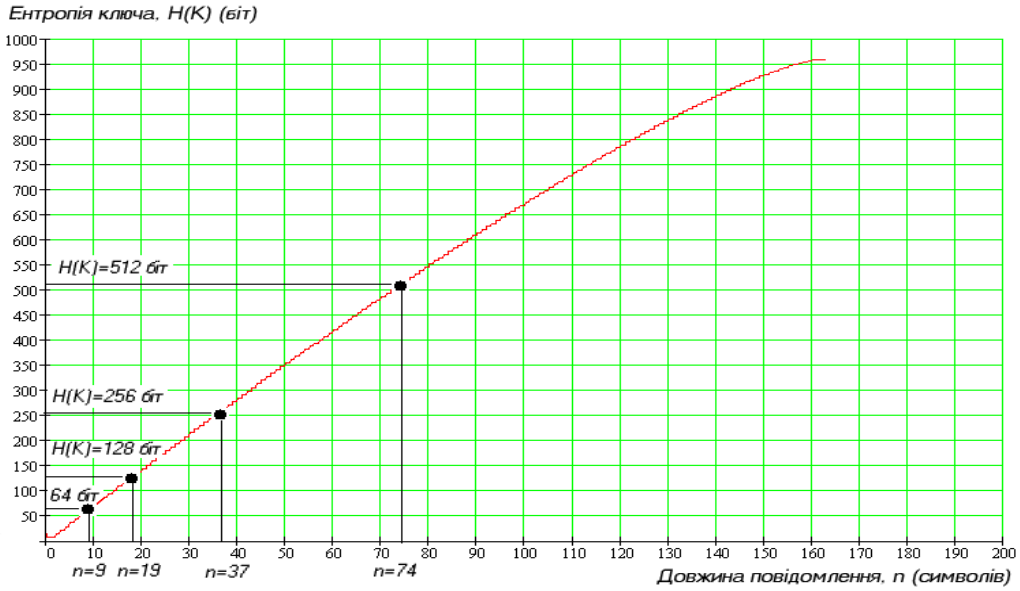


Рис. 2. **Графік залежності ентропії ключа шифру *H(K)* від довжини повідомлення *n***

З графіків на рис. 1 та рис. 2 зробимо наступні висновки. Користувач може задатися сталим розміром ключа шифру, наприклад 64 біти. З графіка на рис. 2 видно, що така довжина ключа шифру відповідає довжині повідомлення у 9 символів (9 рядків для таблиць). З графіка, який зображений на рис. 1, видно, що відстань одиничності, яка відповідає довжині повідомлення, дорівнює $U = 1812$ символів. Таким чином, для того щоб система зберігала властивості досконало секретної при використанні ключа шифру довжиною 64 біти, користувач (передавальна сторона) повинен передавати повідомлення довжиною 9 символів (рядків таблиці) не більше, ніж $\frac{1812}{9} \approx 200$ разів. Іншими словами, користувач повинен змінювати ключ шифру після передавання кожних 200 повідомлень.

Отже, графіки, що зображені на рис. 1 та рис. 2, доцільно використовувати для обчислення максимально можливої кількості сеансів зв'язку без зміни ключа шифру. За таких умов не порушується ознака досконало секретної системи.

Література: 1. Заєць В. В. Проблеми доцільності використання криптостеганографічних методів захисту інформації // Сб. науч. тр. "Защита информации". – 2007. – №14. – С. 103 – 105. 2. Шеннон К. Э. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. – С. 332 – 402. 3. Заєць В. В. Визначення стійкості криптостеганографічних методів захисту інформації / В. В. Заєць, В. М. Чуприн // Зб. наук. пр. Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова. – 2007. – №44. – С. 9 – 19.

Ревак І. О.

УДК [351.746.1+004.853]

ІНТЕЛЕКТУАЛЬНА БЕЗПЕКА – НЕВІД'ЄМНА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Розвиток будь-якої економічної системи є неможливим без сформованої та ефективно діючої системи національної безпеки. В сучасних умовах забезпечення національної безпеки України – це одне із найважливіших та центральних завдань формування й розвитку економіки XXI ст. – економіки знань. Дана проблема не залишає осторонь нашу державу, оскільки перенесення акцентів із матеріальних ресурсів на людські та інтелектуальні є характерним для національної економіки кожної країни та вирішальним у входженні до інформаційного простору. Освіта, наука, інтелект – чинники, що визначають конкурентоспроможність національної безпеки.

Актуальність обраної теми пов'язана, насамперед, з кризовою ситуацією, в якій опинилася вітчизняна наука та освіта. Нинішню ситуацію можна охарактеризувати як таку, якій властиві скорочення обсягів науково-технологічного потенціалу, погіршення таких якісних характеристик, як недостатнє залучення найбільш здібних працівників, наукової молоді до освітньо-наукового сектору національної економіки, соціально-психологічна деградація працівників, моральне та фізичне старіння матеріально-технічної бази НДДКР, зменшення можливостей для відтворення наукових кадрів (складність у системі аспірантури та докторантури), непривабливість наукової кар'єри для молоді, скорочення будівництва науково-дослідних об'єктів, криза наукового приладобудування тощо.

Виокремлюючи інтелектуальну безпеку зі складу національної безпеки, слід наголосити на тому, що інтелектуальна безпека є найменш дослідженим напрямом системи забезпечення національної безпеки.

Проблема забезпечення національної безпеки перебуває в полі зору вітчизняних економістів: О. Данільяна, О. Дзьобаня, М. Панова, Г. Пастернака-Таранушенка, В. Врублевського, В. Ліпкана, Н. Нижника, Г. Ситника, В. Білоуса та ін.

Аналізуючи складові елементи національної безпеки практично всі дослідники виділяють класичні її підвиди: політичну, економічну, воєнну, екологічну, гуманітарну, демографічну, інформаційну [1, с. 12]; економічну, політичну, соціальну, воєнну, екологічну, епідемічну, технологічну, інформаційну [2, с. 55 – 56]; економічну, демографічну, екологічну, продовольчу, військову, ресурсну, прісноводну, енергетичну, цінову, фінансово-грошову, політичну, соціальну, кримінальну, медичну, інформаційну, науково-інтелектуальну [3]. Лише окремі автори акцентують увагу на одній з найважливіших, на думку автора, складовій – інтелектуальній [4, с. 156; 5; 6, с. 11]. Можливо, більшість дослідників цього напряму вбачають в інтелектуальній безпеці якусь менш суттєву складову національної безпеки, або, ймовірніше, розглядають її в складі економічної, технологічної, соціальної чи іншої безпеки.

Метою статті є обґрунтування сутності інтелектуальної безпеки, її складових, внутрішніх і зовнішніх загроз, а також аналіз наукового потенціалу, тенденцій розвитку та заходів, спрямованих на забезпечення інтелектуальної безпеки держави.

Безперечно, інтелектуальна безпека, з одного боку, здатна надто швидко підвищити рівень забезпечення екосестейту через упровадження винаходів, застосування новітніх технологій тощо, а з іншого – надто витратна для держави, яка утримує значну кількість спеціалістів, які після одержання дипломів можуть залишити рідні терени і працювати на економіку інших країн.

Під інтелектуальною безпекою розуміємо стан захищеності всіх продуктів інтелектуальної праці. Перш за все, це продукти інтелектуальної власності, програми, патенти, технології, ліцензії, інформаційні системи тощо, або, іншими словами, все те, що забезпечує прогрес у відтворенні й захисті інтелектуального потенціалу. Безумовно, успішний захист інтелектуальної власності можливий лише за умови чітко відрегульованого та дієвого правового поля. Власник інтелектуального ресурсу не може реально контролювати і захищати свої права, оскільки вітчизняна законодавча база є надто „розмитою", що, без сумніву, зараховує інтелектуальну безпеку до категорії невід'ємної складової національної безпеки держави.

Інтелектуальна складова системи національної безпеки визначається сукупністю соціокультурних, духовних, морально-психологічних, економічних, демографічних, екологічних та інших факторів, які здійснюють відповідний вплив на інтелект нації і кожного громадянина зокрема, формуючи певний світогляд, індивідуальну і суспільну культуру поведінки.

Тлумачення сутності інтелектуальної безпеки є неоднозначним. На думку одних дослідників, інтелектуальна безпека розглядається як захист продуктів інтелектуальної діяльності, інші прирівнюють її до інтелектуальної власності та механізмів її захисту, треті – відносять до інтелектуальної безпеки не тільки захист продуктів інтелектуальної праці, а й раціональне використання, відтворення й підвищення якості розумових здібностей людей, які визначають їх діяльність [6 – 8].

Будь-яка нація, яка не хоче "самознищення" чи підлеглого стану у світовому суспільстві, на думку В. Врублевського, О. Мороза, Ю. Наєнка, передусім має піклуватися про інтелектуальну безпеку, яка включає:

інформаційний самозахист;

психологічну "оборону";

фізичний захист (беруться до уваги фізичні чинники, що визначають інтелектуальне здоров'я народу) [9].

Потрібно звернути увагу на ще один аспект інтелектуальної безпеки – комп'ютерно-інформаційний, оскільки сьогодні з'явилося таке поняття, як інформаційний колоніалізм, що означає перетворення тієї чи іншої країни на "комп'ютерну плантацію". Річ у тому, що інформатизація суспільства визначається не лише кількістю комп'ютерів на певну кількість населення, а й зростанням комп'ютерної грамотності й свідомості населення. Основне завдання державної політики у забезпеченні інтелектуальної безпеки повинно стосуватися використання інтелектуальної праці програмістів, аналітиків, операторів ЕОМ для розв'язання нагальних соціально-економічних проблем та забезпечення прогресивного розвитку сучасного суспільства.

Стан інтелектуальної безпеки держави визначається, перш за все, його науковим потенціалом і науковими ресурсами, тобто кількістю та рівнем підготовки працездатних носіїв наукового інтелекту – осіб, які працюють за здобутим фахом, та осіб з вищою освітою. Враховуючи, що вітчизняна статистика серед видів економічної діяльності виокремлює лише освіту, проаналізуємо зайня-

тість населення в цьому виді діяльності (таблиця). Відомо, що освіта виступає основою та підґрунтям для розвитку наукового потенціалу нації.

Таблиця

Економічна активність населення в освітній сфері*

№ з/п	Показники	2004 р.		2005 р.	
		тис. осіб	%	тис. осіб	%
1	Кількість зайнятого населення,	1 648,7	8,1	1 668,2	8,07
	з них наймані працівники підприємств, установ та організацій	1 643,7	11,7	1 662,0	11,9
2	Кількість звільнених працівників,	5,1	3,7	3,5	2,6
	у тому числі % до передбачених обсягів		21,0		18,7
3	Попит на робочу силу	4,6	2,8	3,9	2,1

* Таблиця складена за даними Статистичного щорічника України [10, с. 372, 378, 380].

Як видно з таблиці, спостерігається тенденція до незначного скорочення кількості зайнятого населення в освітній сфері і при цьому зменшення частки звільнених працівників з освітніх установ і закладів на 1,6 тис. осіб, або 1,1%. Тривожним є факт зниження попиту на осіб, зайнятих в освітній сфері з 4,6 тис. осіб до 3,9 тис., або 0,7%.

У 2005 р. загальна чисельність працівників наукових організацій зменшилася на 1,8% порівняно з 2004 р. і склала 170,6 тис. осіб. Так, частка науковців, що звільнені за скороченням штатів, склала 1 390 осіб (за останні три роки їх число становило 4,4 тис. осіб), у тому числі виконавців науково-технічних робіт – 576. При цьому число науковців, які залишають країну, продовжує зменшуватись: якщо у 2001 – 2004 рр. за кордон виїхали 365 осіб (з них 17 докторів та 90 кандидатів наук), то у 2005 р. – 25 осіб (з них 7 кандидатів наук) [11, с. 30].

Слід зазначити, що скорочення чисельності кадрового потенціалу відбулося за рахунок усіх категорій штатних працівників наукових організацій: дослідників – на 0,6%, техніків – на 2,8%, допоміжного персоналу – на 4,8% – і склало 85,2 тис. осіб, 20,3 тис. осіб і 32,1 тис. осіб відповідно. Одночасно продовжує збільшуватись число працівників-сумісників. У 2005 р. до виконання наукових досліджень і розробок на засадах сумісництва було залучено 68,5 тис. науково-педагогічних працівників вищих навчальних закладів та інших спеціалістів, що на 4,5% більше, ніж у 2004 році.

У різних галузях економіки на 1 жовтня 2005 року працювало 80,3 тис. докторів і кандидатів наук, з яких 26,4% виконували наукові дослідження й розробки за основним місцем роботи, майже 35% – працівники, які поєднували викладацьку діяльність у вищих навчальних закладах з науковою.

При загальній тенденції скорочення чисельності виконавців наукових досліджень і розробок спостерігається поступове зростання питомої ваги фахівців із науковими ступенями. Так, у 2000 р. їх частка становила 18,2%, у 2003 р. – 19,8%, у 2005 р. – 20,1% і склала 21,2 тис. осіб (4,1 тис. докторів та 17,0 тис. кандидатів наук) [11].

Із упевненістю можемо стверджувати, що інтелектуальна безпека – це такий стан національної безпеки, який дозволяє зберігати стійкість до внутрішніх і зовнішніх загроз та здатний задовольняти потреби всіх суб'єктів – особи, сім'ї, суспільства та держави. До основних реальних та потенційних (внутрішніх і зовнішніх) загроз інтелектуальній безпеці суспільства можна віднести: недостатній рівень фінансування освіти та науки; заниження соціальної значущості вчених і спеціалістів із вищою освітою; моральна і матеріальна недооцінка державою праці науковців; непрестижність наукоємних професій; нестабільність роботи науково-дослідних установ; використання вчених і спеціалістів із вищою освітою не за здобутим фахом; старіння й нестача наукових кадрів; низький рівень заробітної плати в освітній та науковій сферах, відсутність належної мотивації до праці; погіршення фізичного та духовного здоров'я населення, моральна деградація особи, сім'ї, суспільства; зростаюче науково-технологічне відставання України від розвинутих держав світу; інтелектуальна міграція та ін.

Забезпечення інтелектуальної безпеки держави можливе за рахунок розвитку наукоємних галузей економіки, впровадження новітніх технологій (нанотехнологій, штучного інтелекту), використання досягнень науки і техніки у виробництві (забезпечення тріади: освіта – наука – виробництво), можливості рівного доступу до отримання освіти всіх членів суспільства, використання набутих знань, вмінь та навичок у створенні продуктів інтелектуальної праці, забезпечення безперервної освіти й перепідготовки кадрів, створення науково-освітніх комплексів (центрів) або корпоративних університетів, надання якісної вищої освіти (в контексті Болонської декларації з використанням кредитно-модульної системи), підвищення привабливості академічної кар'єри для випускників вищих навчальних закладів, забезпеченості й захисту прав на інтелектуальну власність та ін.

Очевидно, що для забезпечення і зміцнення інтелектуальної безпеки України необхідно реалізувати комплекс організаційно-правових, господарсько-економічних та інших заходів, спрямованих не тільки на збереження і відтворення існуючого інтелектуального потенціалу, а й на підвищення престижності розумової праці, зацікавленості носіїв наукового інтелекту у плідній праці. Таким чином, нова парадигма розвитку і нарощування інтелектуального та науково-технологічного потенціалу допоможе знизити й усунути низку потенційних і реальних загроз інтелектуальній безпеці, а також забезпечить вищий ступінь захисту національної безпеки в цілому.

Під інтелектуальним захистом розуміють заходи, спрямовані на забезпечення інтелектуальної безпеки держави. Безумовно, заходи, пов'язані з попередженням загроз інтелектуальним інтересам[1], слід вважати пасивним захистом або пасивним забезпеченням інтелектуальної безпеки. Ті ж заходи, які направлені на обмеження й ліквідацію наслідків небезпек інтелектуальним інтересам, що виникли, можна вважати активним захистом або активним забезпеченням інтелектуальної безпеки.

До заходів пасивного захисту можна віднести: розробку сучасної концепції науково-технічної політики, розвитку науки й освіти, яка б відповідала новим соціально-економічним умовам розвитку країни; розробку законів, законодавчих та нормативних актів, які б забезпечували і стимулювали розвиток науки та освіти; розробку законів і законодавчих актів, які б захищали інтелектуальні інтереси країни, інтелектуальну власність, носіїв інтелектуальної власності та продукти їх розумової праці; розробку вимог до дипломних і випускних робіт, дисертацій на здобуття наукових ступенів тощо.

До заходів активного впливу можна віднести: практичну реалізацію інтелектуальних можливостей особи, сім'ї, суспільства, держави; зростання суспільної та соціальної значущості спеціалістів із вищою освітою і вчених при розробці нормативних актів та розв'язанні державних і інших завдань; покращення умов праці та життя носіям інтелекту − вченим і спеціалістам із вищою освітою; реальний захист продуктів розумової діяльності носіїв інтелекту від різного роду посягань; використання вчених і спеціалістів з вищою освітою тільки за профілем їх підготовки; моральне та матеріальне стимулювання роботи носіїв інтелекту; швидке впровадження й застосування результатів діяльності вчених і спеціалістів з вищою освітою на практиці та ін.

Вивчення, аналіз й оцінка вищезгаданих проблем, на погляд автора, є надзвичайно перспективним напрямом наукового дослідження. Україна має значний інтелектуальний потенціал, який потребує ефективного та належного використання, що, у свою чергу, забезпечить інтелектуальну безпеку держави.

Отже, інтелектуальна безпека є невід'ємною складовою частиною національної безпеки, оскільки забезпечує задоволення інтелектуальних інтересів особи, суспільства та держави; гарантує належні умови для цивілізованого життя, розвитку та вдосконалення; визначає наукове забезпечення й реалізацію всіх інших видів національної безпеки; виступає важливим чинником збереження та примноження інтелекту нації; гарантує недопущення інтелектуальної кризи, яка може виявитися надзвичайно небезпечною порівняно з економічною, соціальною, воєнною й подолання якої потягне декілька десятиліть або й століть. Багатоаспектність, складність, масштабність і глибина проблеми розвитку і збереження інтелекту виводить забезпечення інтелектуальної безпеки країни в категорію найактуальніших проблем сучасності.

Література: 1. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації. Навч. посіб. / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. – Харків: Фоліо, 2002. – 284 с. 2. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус; [За заг. ред. П. В. Мельника, Н. Р. Нижник. – Ірпінь, 2000. – 304 с. 3. Пастернак-Таранушенко Г. А. Економічна безпека держави. Методологія забезпечення: Монографія. – К.: Київський економічний інститут менеджменту, 2003. – 320 с. 4. Берлач А. І. Основи економічної безпеки України: Навч. посіб. / А. І. Берлач, Т. В. Філіпенко. – Донецьк: Донецький юридичний інститут ЛДУВС ім. Е. О. Дідоренка, 2007. – 236 с. 5. Дубровин И. Р. Интеллектуальная безопасность / И. Р. Дубровин, Е. Р. Дубровин // МОСТ. – 2004. – №57. – Январь. 6. Пирумов В. С. Некоторые аспекты методологии и исследования проблем национальной безопасности России в современных условиях // Геополитика и безопасность. – 1993. – №1. – С. 7 – 17. 7. Лебедько В. Г. Прогнозная оценка изменения геополитической картины мира в районах "дальнего зарубежья" // Геополитика и безопасность. – 1993. – №1. – С. 18 – 75. 8. Чернявский Г. С. К вопросу исследования проблем безопасности России // Военная мысль. – 1994. – №9. – С. 2 – 8. 9. Врублевський В. Інтелектуальний капітал як головна продуктивна сила / В. Врублевський, О. Мороз, Ю. Саєнко // www.universum.org.ua 10. Статистичний щорічник України за 2005 рік – К., 2006. – 575 с. 11. Наукова та інноваційна діяльність в Україні. Стат. збірник / Відп. за випуск І. В. Калачова. – К., 2006. – 364 с.

---

[1] До інтелектуальних інтересів нації відносимо збереження та розвиток інтелектуального й науково-технологічного потенціалу України; проведення модернізації національного виробництва та розвиток його наукоємних галузей; розвиток духовності, моральних засад, зміцнення фізичного здоров'я, створення умов для розширеного відтворення населення. Особлива роль у системі інтелектуальних інтересів належить науковому інтелекту, оскільки саме він визначає рівень розвитку суспільства, його духовну міць та авторитет.

Дудикевич В. Б.

Максимович В. М.

Костів Ю. М.

УДК 681.3

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ МОДИФІКОВАНОГО ГЕНЕРАТОРА ДЖІФФІ

У зв'язку з упровадженням новітніх технологій у системах захисту інформації значно розширилась сфера застосування генераторів випадкових і псевдовипадкових імпульсних послідовностей, що ставить нові вимоги до їх проектування та методів оцінки якості.

У даній роботі запропонований спосіб збільшення періоду повторення псевдовипадкової послідовності чисел, що є одним з основних параметрів генератора псевдовипадкових чисел (ГПЧ), який ґрунтується на використанні модифікованого генератора Джіффі.

Одним із найефективніших і найбільш швидкодіючих методів отримання псевдовипадкових рівномірно розподілених чисел є їх генерування на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (Linear Feedback Shift Register). Один із найбільш відомих генераторів на основі LFSR – генератор Джіффі [1; 2], який забезпечує перемішування двох послідовностей x_1 і x_2 з виходів LFSR 1 і LFSR 2 під управлінням послідовності x_3 з виходу LFSR 3. Перемішування здійснюється за допомогою функції ускладнення:

$$F(x_1, x_2, x_3) = x_1\overline{x_3} + x_2x_3 = x_3 \oplus x_1x_2 \oplus x_2x_3, \tag{1}$$

яка може бути реалізована за допомогою мультиплексора 2 → 1. Якщо LFSR мають розрядність N_1, N_2, і N_3, то лінійна складність генератора рівна

$$LC = N_1(N_3 + 1) + N_2N_3. \tag{2}$$

У тому випадку, коли періоди S_i послідовностей $\{x_i(t)\}$ попарно взаємно прості, період результуючої послідовності γ(t) дорівнює добутку $S_1S_2S_3$. Функція F видає на вихід інформацію про стан LFSR 1 і LFSR 2, бо ймовірність збігу елемента вихідної послідовності із значенням x_1 або x_2 рівна 3/4, інакше кажучи,

$$P(F(x_1,x_2,x_3) = x_1) = P(F(x_1,x_2,x_3) = x_2) = 3/4. \tag{3}$$

Можливі інші варіанти даної схеми. Так, наприклад, використання виразу

$$F(x_1,x_2,x_3) = x_1x_3 \oplus x_1x_2 \oplus x_2x_3 \tag{4}$$

дозволяє отримувати послідовності з більш високою лінійною складністю:

$$LC = N_1N_2 + N_1N_3 + N_2N_3. \tag{5}$$

При поточному *n*-розрядному шифруванні можна добитися більш ефективного перемішування двох *n*-розрядних псевдовипадкових послідовностей за рахунок використання функції ускладнення на основі *n* 1-розрядних мультиплексорів 2 → 1.

У роботі наведені результати дослідження модифікованого генератора Джіффі (рис. 1), який відрізняється від відомого [2] тим, що з виходів LFSR 1 і LFSR 2 знімаються паралельні коди псевдовипадкових чисел, керування мультиплексором реалізується послідовним псевдовипадковим кодом з виходу LFSR 3 і, таким чином, на виході генератора формується псевдовипадкова послідовність чисел.

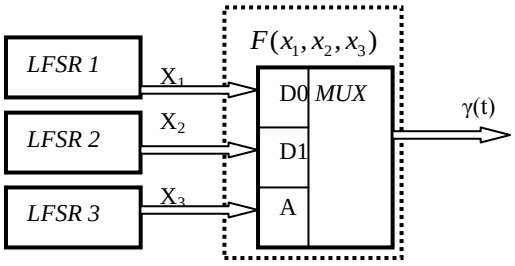


Рис. 1. **Модифікований генератор Джіффі**

Дослідження проводились за допомогою програми, створеної для оцінки якості послідовності псевдовипадкових чисел. При цьому використовували групу тестів, до якої входять графічні й оціночні тести.

У результаті виконаного аналізу існуючих тестів виявлено, що дослідження та оцінку якості послідовності псевдовипадкових чисел можна оцінити за допомогою графічного тесту "розподіл на площині " та наступного ряду оціночних тестів: перевірка кореляції; перевірка перестановок, що пересікаються; перевірка на монотонність; перевірка перестановок; тест дірок; перевірка незчіплених серій; частотний монобітний тест [3; 4].

Запропоновано застосовувати різні тести саме для того, щоб з найбільшою вірогідністю зробити висновок про придатність базового ГПЧ для подальшого використання.

У процесі роботи були досліджені різні варіанти побудови модифікованого генератора Джіффі:

а) для різних примітивних поліномів генератора М-послідовності, які є в основі LFSR 1, LFSR 2, LFSR 3. Послідовності чисел x_1 і x_2 отримували з генераторів М-послідовностей, реалізованих на примітивних поліномах степеня N = 17: $\Phi(x) = 1 \oplus x^{12} \oplus x^{17}$, $\Phi(x) = 1 \oplus x^{6} \oplus x^{17}$; послідовність x_3 з виходу генератора М-послідовностей степеня N=7: $\Phi(x) = 1 \oplus x^{6} \oplus x^{7}$; а також на примітивних поліномах степеня N = 31: $\Phi(x) = 1 \oplus x^{18} \oplus x^{31}$, $\Phi(x) = 1 \oplus x^{24} \oplus x^{31}$, при керуючому генераторові, побудованому на згаданому вище поліномі степеня N = 7;

б) при різних степенях матричних рівнянь (r − степінь, до якого підноситься квадратна матриця), що описують роботу генератора М-послідовності. На рис. 2 і рис. 3 показано генератори М-послідовності при степені матричних рівнянь 1 і 10 відповідно на основі твірного полінома $1 + x^{18} + x^{31}$.

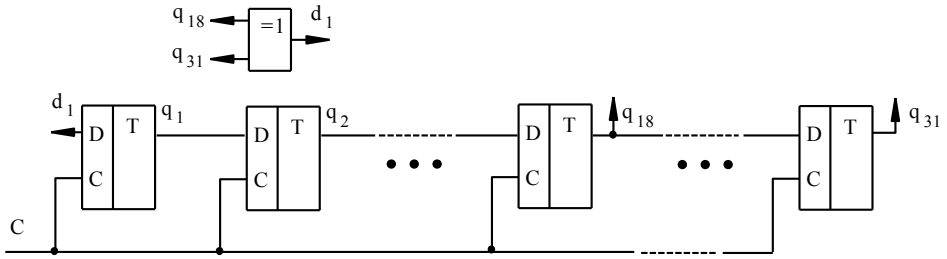


Рис. 2. **Генератор М-послідовності на основі твірного поліному $1+x^{18}+x^{31}$ для матриці T_1 при $r=1$**

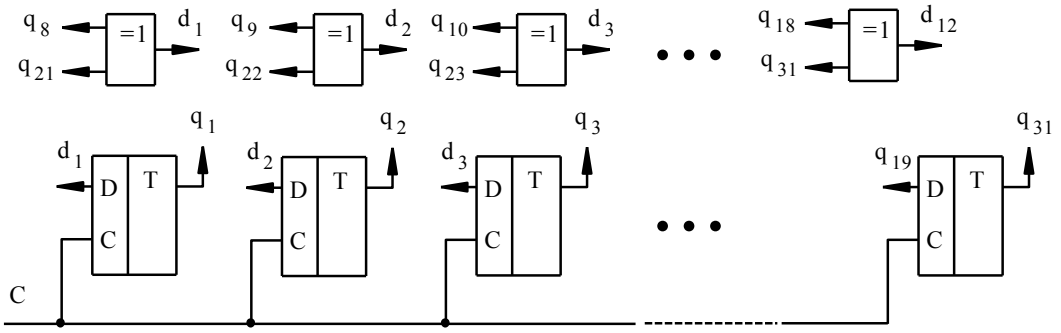


Рис. 3. **Генератор М-послідовності на основі твірного поліному $1+x^{18}+x^{31}$ для матриці T_1 при $r=10$**

У результаті проведеного моделювання роботи модифікованого генератора Джіффі та оцінки його якості було доведено, що при значенні степеня матриці r = 10 досягається найвища якість його роботи. При значеннях r < 10 послідовності на виході модифікованого генератора Джіффі пройшли не всі тести, за допомогою яких проводилось оцінювання. При значеннях r > 10 результати оцінювання були практично подібними до результатів оцінювання при r = 10, але при цьому ускладнювалась апаратна реалізація побудови даних генераторів.

Для кращого оцінювання якості та з метою використання в деяких тестах кожна послідовність, що генерується, розбивається на інтервали, максимальна кількість яких визначається як n_{max} (у діапазоні від 1 до n_{max}), у свою чергу кожен інтервал розбивається на підінтервали, максимальне значення яких визначається як i_{max} (у діапазоні від 1 до i_{max}).

Основною умовою, яка повинна дотримуватись при розбитті на інтервали, є те, що добуток $n_{max} \cdot i_{max}$ повинен бути меншим за період.

Результати оціночного тестування модифікованого генератора Джіффі при i_{max} = 10000, n_{max} = 100 і степені матриці r = 10 наведено в таблиці.

Таблиця

Результати оціночного тестування

Вид оціночного тесту	Результат
Перевірка перестановок, що пересікаються	пройдено
Перевірка перестановок	пройдено
Перевірка незціплених серій	пройдено
Перевірка на монотонність	пройдено
Перевірка кореляції	пройдено
Частотний монобітний тест	пройдено
Тест дірок	пройдено

Таким чином, при побудові модифікованого генератора Джіффі, залежно від конкретного випадку застосування, доцільно використовувати для його побудови структури на основі примітивних поліномів, що забезпечують потрібний період повторення, а параметр r доцільно вибирати рівним чи близьким до 10, оскільки саме при таких значеннях були отримані задовільні характеристики псевдовипадкових послідовностей чисел.

Література: 1. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ – ОБРАЗ, 2003 – 240 с. 2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ – ОБРАЗ, 2001. – 368 с. 3. Гарасимчук О. І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / О. І. Гарасимчук, В. М. Максимович // Захист інформації. – №3. – 2003. – С. 29 – 36. 4. Гарасимчук О. І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей / О. І. Гарасимчук, В. М. Максимович // Вісник Національного університету "Львівська політехніка" "Комп'ютерні науки та інформаційні технології". – 2004. – №521. – С. 17 – 23.

Шарапов В. Г.

УДК 681.3.06

МОДИФІКОВАНИЙ АЛГОРИТМ ТЕСТУВАННЯ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ З ВИКОРИСТАННЯМ КОНТЕКСТНОГО МОДЕЛЮВАННЯ

Серед множини різних тестів перевірки якості випадкових і псевдовипадкових послідовностей особливу групу становлять тести, засновані на стисненні інформації [1].

Згідно з джерелом [2] двійкова послідовність s, $s \in \{0,1\}^n$, $n \in \mathrm{N}$ буде непередбаченою, якщо для довільного поліноміального ймовірнісного алгоритму A виконується наступна умова. Нехай $l\varsigma$ – деякий префікс послідовності S (тобто перші k біт), де $\varsigma \in \{0,1\}$, $l \in \{0,1\}^{k-1}$, l – префікс довжини $k-1$, а k – це випадкове натуральне число, яке не перевищує n. Тоді

$$\left| \mathrm{P}[A(l) = \varsigma] - \frac{1}{2} \right| < \frac{1}{n^c} \qquad (1)$$

для кожного c при досить великих n.

Запишемо умову (1) менш формально. Послідовність не є випадковою, якщо, аналізуючи цю послідовність зліва-направо і накопичуючи при цьому інформацію, ми отримуємо можливість прогнозувати наступні символи. Послідовність є випадковою, якщо вона не ідентифікована як невипадкова.

Розглянемо деякий поліноміальний імовірнісний алгоритм A, в якому має місце двійковий рядок s, $s \in \{0,1\}^n$, $n \in \mathrm{N}$, такий, що $s = l\varsigma$, $l \in \{0,1\}^{n-1}$, $\varsigma \in \{0,1\}$. Будемо називати прогнозом n-го символу $A(l)$ і говорити, що:

символ ς — передбачено, якщо $A(l) = \varsigma$;

символ ς — непередбачено, якщо $A(l) \neq \varsigma$;

символ ς — непередбачуваний, якщо $A(l)$ не визначено.

При побудові критерію було використано такі визначення й положення:

будь-який символ, що знаходиться в рядку, безпосередньо йде за деяким підрядком, можливо порожнім. Такий підрядок називається *контекстом* [2] символу;

порядок контексту – це довжина підрядка.

Критерій реалізується за допомогою алгоритму, результатом роботи якого є кількість передбачених, непередбачених і непередбачуваних символів.

Підрахунок та класифікації прогнозованих символів

Постановка задачі

Припустимо, що маємо двійкову послідовність s довжини n. Для кожного символу s_i, $i = \overline{1,n}$, маємо набір контекстів $X_i = \{x_i^{(j)}\}$, $j = \overline{0, \min\{M, i-1\}}$, де M – максимальний порядок контексту,

$$x_i^{(j)} = \begin{cases} s_{i-j} \ldots s_{i-2} s_{i-1}, & \text{для } j \geq 1; \\ \text{""}, & \text{для } j = 0 \end{cases}$$

Необхідно визначити кількість передбачених, непередбачених і непередбачуваних символів, обмежуючи порядок контекстів, що розглядаються значенням $M \in N$.

Тоді неформальний алгоритм підрахунку передбачуваності символів у рядку можна визначити наступним чином:

Алгоритм 1.

1. Для кожного контексту $x_i^{(j)}$ з набору X_i символу s_i обчислити кількість входжень $p_i^{(j)}$ до всіх наборів контекстів попередніх символів рядку, що збігаються з поточним символом s_i:

$$p_i^{(j)} = \sum_{x_i^{(j)} \in X_k,\ s_k = s_i} 1 \quad , \text{ де } k = \overline{1, i-1}.$$

2. Для кожного контексту $x_i^{(j)}$ з набору X_i символу s_i обчислити кількість входжень $q_i^{(j)}$ до всіх наборів контекстів попередніх символів рядка, що не збігаються з поточним символом s_i:

$$q_i^{(j)} = \sum_{x_i^{(j)} \in X_k,\ s_k \neq s_i} 1 \quad , \text{ де } k = \overline{1, i-1}.$$

3. Для кожної пари кількості входжень обчислити

$$\rho_i^{(j)} = p_i^{(j)} - q_i^{(j)}.$$

4. Якщо $\max\limits_j \left| \rho_i^{(j)} \right| \leq 1$, то s_i – непередбачуваний символ і перейти до п. 6.

5. Символ s_i передбачений, якщо $\rho_i^{(k)} > 1$, та непередбачений у протилежному випадку, де $k = \max\limits_{\left|\rho_i^{(j)}\right| > 1} j$.

6. Виконувати пункти 1 – 5, поки $i = \overline{1, n}$.

Практичні випробування

Для перевірки придатності алгоритму було виконано багато перевірок випадкових, псевдовипадкових та невипадкових послідовностей. Експерименти показали, що генератори побудовані на основі стійких блочних шифрів, наприклад AES, дуже добре себе ведуть і показують результати, дуже близькі до фізичних.

Експерименти показали, що:

при використанні контексту 6-го та більших порядків різниця між кількістю правильно та неправильно передбачених символів, $c_r - c_w$, для випадкової послідовності буде нормально розподіленою з математичним очікуванням 0;

середньоквадратичне відхилення залежить як від довжини послідовності, так і від порядку контексту. Значення відображені на рис. 1 − 3. Для невипадкової послідовності ця величина буде додатною.

Критерій оцінки якості випадкової послідовності

Суть критерію полягає в тому, що для вхідної послідовності обчислюються величини c_r, c_w, c_u. А потім виконується перевірка на відповідність величин c_u та $c_r - c_w$ нормальному розподілу з експериментально отриманими параметрами.

Для перевірки того, чи є надана послідовність послідовністю рівноймовірних біт, необхідно скористатися наведеним нижче алгоритмом.

Вхідні дані:

порядок контексту M;

вхідна двійкова послідовність S довжини m (m не менше 48);

рівень значущості критерію − б.

Вихідні дані:

відповідь на те, задовольняє вхідна послідовність критерій із заданою ймовірністю чи ні.

Для перевірки послідовності необхідно виконати наступні кроки.

1. Якщо $m < 48$, то завершити тест із помилкою "надана послідовність занадто мала для застосування тесту".

2. Обчислити c_r, c_w, c_u.

3. Перевірити з заданим рівнем значущості $c_u \sim N(u_{M(n)}, u_{D(n)})$:

$$\left| \frac{c_u - u_{M(n)}}{\sqrt{u_{D(n)}}} \right| \le u_{1-\alpha/2},$$

де u_q − квантиль стандартного нормального розподілу рівня q.

4. Перевірити з заданим рівнем значущості $c_r - c_w \sim N(0, c_r + c_w)$:

$$\left| \frac{c_r - c_w}{\sqrt{c_r + c_w}} \right| \le u_{1-\alpha/2}.$$

5. Якщо виконуються нерівності на етапах 3 та 4, то вхідна послідовність *пройшла* тест із заданою ймовірністю, інакше послідовність тест *не пройшла*.

Рекомендований до використання рівень значущості для тесту 0,5 та більше.

Деякі результати практичних випробувань послідовностей різної довжини наводяться на рис. 1 − 3. На осі абсцис відображається різниця між кількістю правильно та неправильно передбачених символів, а по осі ординат − кількість послідовностей.

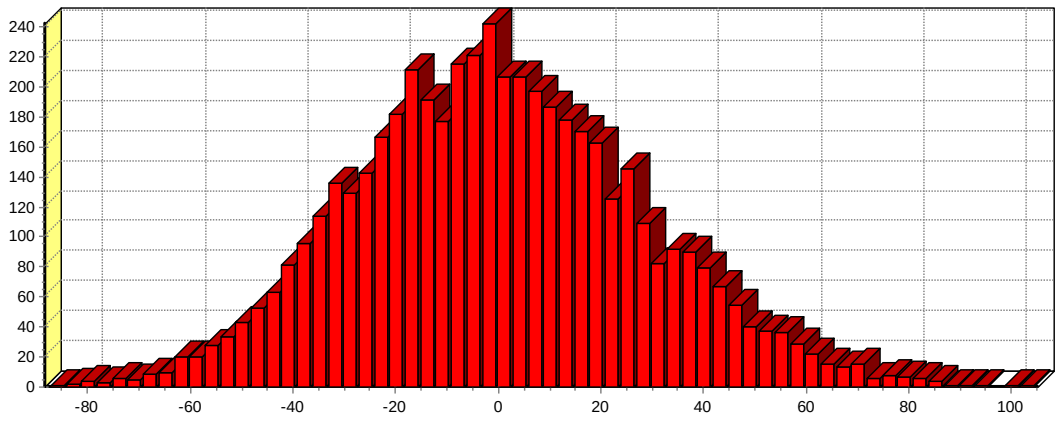


Рис. 1. **Довжина 1 024 біти, максимальний порядок контексту 20**

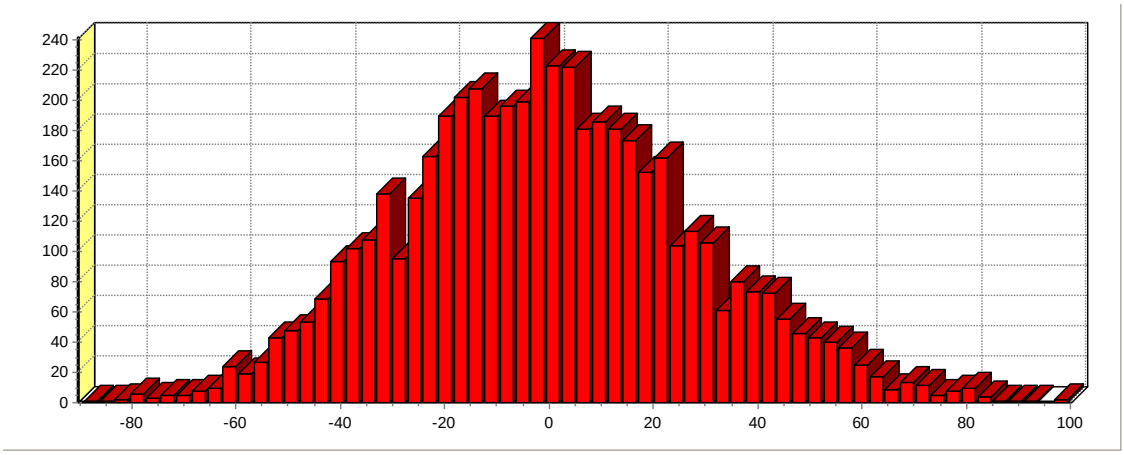


Рис. 2. **Довжина 1 024 біти, максимальний порядок контексту 8**

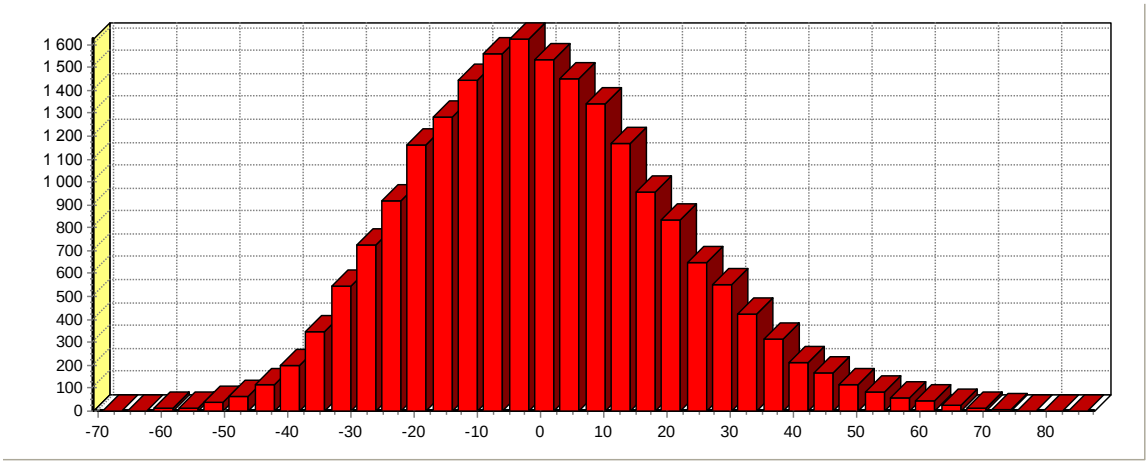


Рис. 3. **Довжина 512 біт, максимальний порядок контексту 8**

Для побудови рис. 1 та 2 використовувалась послідовність, отримана шляхом шифрування блочним шифром AES великого файла з відеозображенням. На рис. 3 показано результати аналізу послідовності, отриманої від модулярного генератора псевдовипадкових величин, зі стандартної бібліотеки Delphi. Розмір вибірок – 10 000.

Основними перевагами поданого алгоритму є те, що він ефективний навіть для дуже коротких послідовностей та надає чисельний результат для будь-яких вхідних даних незалежно від їх випадковості.

Порівняно з попередніми версіями з алгоритму відкинуто врахування кількості правильних та неправильних прогнозів, зроблених раніше. Тепер достатньо, щоб це число було додатнім, а саме значення не має різниці. Також не виконується обчислення складної узагальнюючої функції, а використовуються різниці між кількостями спрогнозованих символів.

Коди програм, що реалізують вказаний алгоритм та його модифікації, а також експериментальні дані знаходяться на сайті http://cryptonews.org.ua/VSharapov/

Література: 1. Шарапов В. Тестирование случайных и псевдослучайных последовательностей с использованием контекстного моделирования // Наук.-техн. зб. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – 2007. – Вип. 2.(15). – С. 86 – 97. 2. Вербіцький О. В. Вступ до криптології. – Львів: ВТНЛ, 1998. – 250 с. 3. Ватолин Д. Методы сжатия данных. Устройства архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ-МИФИ, 2003. – 384 с.

Васильєва А. А.

Місюра А. О.

УДК 004.056.5

СИСТЕМИ МОНІТОРИНГУ ТА ЗАПОБІГАННЯ АТАК У МЕРЕЖАХ ЗКС-7

Система сигналізації за загальним каналом ЗКС-7 є одним з найважливіших об'єктів експлуатаційного управління мереж зв'язку загального користування. Вона забезпечує засоби сигналізації та управління каналами не тільки в телефонних, інтелектуальних і ISDN-мережах, а й у мережах мобільного зв'язку всіх існуючих і перспективних стандартів, а також при взаємодії вищеперелічених мереж з мережами VoIP. Система ЗКС-7 володіє рядом переваг порівняно з традиційними системами сигналізації. Це висока швидкість встановлення з'єднання та висока продуктивність, економічність і універсальність, можливість модернізації окремих компонентів протоколу та гнучка реконфігурація сигнального трафіка [1].

Бурхливі темпи розвитку мереж зв'язку дозволяють передбачити, що найближчим часом мережа ЗКС-7 буде використовуватися для управління половиною телефонного трафіка країни, так що зупинка роботи цієї мережі може мати катастрофічні наслідки. Оскільки обсяг сигнального трафіка й складність мереж сигналізації постійно зростають, для підтримки належного рівня якості надання сучасних послуг операторам мереж необхідно постійно мати повний контроль над їх мережами ЗКС-7 [2].

Проблема забезпечення надійності мережі ЗКС-7 є важливою для кожного оператора зв'язку, а також служб національної безпеки, оскільки збій у роботі будь-якої мережі може призвести до відмов роботи критичних точок економіки країни. Причини виникнення цієї проблеми наступні:

протокол сигналізації спроектований для замкнутої мережі, в якій обмін інформацією відбувається лише між самими автоматичними телефонними станціями (АТС) або між АТС та мережними базами даних;

у протоколі сигналізації відсутні процедури аутентифікації та шифрування, тобто контролю доступу;

наявність ненавмисних порушень (перевантаження, розповсюдження відмов) і навмисних порушень безпеки мережі сигналізації (маскування, порушення цілісності даних про ресурси сигналізації, моніторинг та розкриття важливої інформації).

Докладно загрози порушення безпеки мереж сигналізації за загальним каналом та можливі наслідки наведено в роботі [2].

Досліджена модель порушника вказує на необхідність побудови загальнодержавної системи безпеки мереж ЗКС-7.

Технічні підходи, розроблені для захисту мереж ЗКС-7, можна поділити на дві групи.

Перша група передбачає особливу організацію мережної архітектури та включає такі методи, як:

обмеження точок взаємодії з мережами VoIP за рахунок централізації ланок доступу з їх сторони;

фізичне розділення сигнального й голосового трафіка на міжмережних інтерфейсах;

захист доступних через інтерфейси експлуатаційного управління АТС внутрішньостанційних даних за допомогою багаторівневої системи паролів.

Друга група підходів передбачає використання додаткових спеціалізованих програмно-апаратних засобів для перевірки сигнальних повідомлень за допомогою "мережних екранів" та/або для пасивного моніторингу за допомогою систем централізованого аналізу й реагування на атаки.

Застосування методів захисту тільки з однієї групи не дає позитивного результату, у зв'язку з чим у більшості випадків потрібне вживання хоча б одного методу з обох груп.

Об'єктом дослідження в статті є друга група підходів, а саме існуючі розподілені системи моніторингу та фрод-контролю. Принцип їх побудови заснований на підключенні до ланок мережі ЗКС-7 моніторів, які направляють до центру спостереження сигнали попередження про раптове збільшення або зменшення сигнального трафіка, тим самим попереджають про можливі атаки. Повідомлення попередження генеруються системою за умови перевищення порогу навантаження, який є нормою для мережі в цілому або для кожної з її ланок. Це повідомлення супроводжується інформацією про джерело, час виникнення та тип потенційно небезпечної події.

Застосування таких систем вимагає чималих витрат, але й переваги, що надаються розподіленими системами, стають усе більш суттєвими останнім часом (табл. 1).

Таблиця 1

Плюси та мінуси застосування розподілених систем моніторингу

Витрати	Переваги
Додаткові апаратні та програмні засоби	Зменшення кількості обслуговуючого персоналу за рахунок автоматизації і віддаленого управління системою
Ресурси мережі передавання даних між видаленими модулями та центром спостереження	Зменшення часу простою ресурсів за рахунок швидкого виявлення відмов та автоматичного повідомлення
Розробка специфічних функцій для кожного замовника системи, пусконалагоджувальні роботи	Виявлення та аналіз тенденцій, що впливають на якість функціонування обладнання шляхом статичної обробки інформації
	Віддалений доступ до додатків у результаті уніфікації інтерфейсу між віддаленими модулями та центром нагляду
	Додаткові прибутки внаслідок своєчасного виявлення "сірих схем" проходження трафіка

Запропоновані на світовому ринку системи моніторингу схожі за своїми функціями, тобто надають майже однаковий мінімальний набір можливостей. Однак найбільш цікавими з поданих є системи, які наведено в табл. 2 [3].

Таблиця 2

Переваги та недоліки найбільш відомих систем моніторингу

Назва системи, виробник	Переваги	Недоліки	
"Access", Agilent (США)	Зручний інтерфейс користувача. Авторитетна компанія	Застаріла технологія. Ускладнене розширення. Відомі випадки незадоволеності клієнтів. Немає установок у СНД	Англомовний інтерфейс. Немає обліку особливостей російських та українських специфікацій ЗКС
"Geo Probe" Tektronix (США)	Фактичний лідер на ринку США	Застаріла технологія. Обмежений обсяг інформації, що приймається, та високі вимоги до однорідності мережі. Незручний інтерфейс користувача. Немає установок у СНД	
"Nexus" Nexus Telecom (Швейцарія)	Сумісна за форматами з аналізаторами Tektronix. Одна з найстаріших розробок систем такого класу	Застаріла технологія. Великі малогабаритні показники. Немає установок у СНД	
"Master Quest" NetTest (Данія)	Сумісна з платформою TeMIP DEC. Орієнтована на TMN-підхід	Технологія локальних аналізаторів. Надмірність функцій	
"Fraud View", ECTel (Ізраїль)	Клієнтське програмне забезпечення під Windows. Менеджер задач. Апробація у великій кількості проектів. Установки в Росії	Немає функції побітового декодування повідомлень. Немає функцій контролю стану ланок та вимірювання навантаження. Незручний інтерфейс користувача. Недостатньо гнучка система конфігурації	
"WWG 8620 SS7" Acterna (Німеччина)	Клієнтське програмне забезпечення під Unix або Windows. Можливість розподілення модулів та нарощування. Широкий спектр стандартних протоколів і місцевих варіацій	Високі вимоги щодо однорідності мережі. Немає установок у СНД	
"Спайдер" НТЦ "Севен Тест" (Росія)	Сумісна з платформою тестерів SNT. Досвід установлення різними операторами з ISUP-R і R1.5. Адаптація та місцева технічна підтримка 24x7	Промислова експлуатація великих систем тільки з 2001 р. Обмежені маркетингові можливості. Відсутність установок за кордоном	
"Сапсан" ИВП "Инно Винн" (Україна)	Зручний інтерфейс користувача. Оптимальне співвідношення "ціна – якість". Орієнтованість на використання в країнах СНД. Досвід установок в Україні та Росії		

Детальну інформацію щодо основних функцій, особливостей архітектури, програмного забезпечення, результатів упровадження наведених систем моніторингу ЗКС-7 та основної клієнтської бази фірм-виробників наведено на їх сайтах (наприклад, джерела [4 – 6]).

Проведений аналіз існуючих систем моніторингу ЗКС-7 з точки зору гнучкої архітектури, що задовольняє вимоги до організації моніторингу в кожному з філіалів окремо та централізованого контролю з головного офісу, а також до інтерфейсу з системами управління та білінгу, вказує, що найбільш відповідними для роботи в країнах СНД є системи "Спайдер" і "Сапсан". Підтвердженням цього є їх надійність, швидкодія, багатофункціональність, значні можливості фільтрації, моніторинг із різним рівнем деталізації, самоконтроль, зручний інтерфейс та велика кількість відомих фірм-клієнтів (для "Спайдер" це "Golden Telecom" (Москва, Санкт-Петербург), "Арктел" (Москва, Санкт-Петербург, Самара, Хабаровськ та ін.), "Комстар" (Москва), "Дальсвязь" (Южно-Сахалінськ) та інші, а для "Сапсан" – ВАТ "Укртелеком", ВАТ "РЕКОМ" (МТС, Росія), оператор міжнародного зв'язку "Utel" (Україна)). Треба зазначити також спроможність використання наведених систем у мережах зв'язку наступного покоління NGN [7].

Література: 1. Прозоров В. М. Общеканальная система сигнализации №7. Учеб. пособие. Ч. 1: Подсистема передачи сообщений / В. М. Прозоров, А. И. Стебленко. – Ижевск: Изд. ИжГТУ, 2003. – 88 с. 2. Гольдштейн Б. С. Обеспечение безопасности сетей ОКС-7 / Б. С. Гольдштейн, И. М. Ехриель, Р. Д. Рерле // Сети связи. – №7. – 2007. – http://www.seventest.ru/docs/SS7_security2.pdf. 3. Королёв В. Системы мониторинга сети сигнализации как базовая составляющая OSS/BSS компаний-операторов // Connect! Мир Связи. – №7. – 2007. – http://www.seventest.ru/docs/korolev.pdf. 4. http://www.vilcomspb.ru/kommyt /8620_nabl.html. 5. http://www.-seventest.ru. 6. http://www.innovinn.com/home.php. 7. Исаченко Ю. С. Анализаторы протоколов для NGN // Вестник связи. – №9. – 2006. – www.niits.ru/public/2006/2006-039.pdf.

Жученко А. С.

Лысечко В. П.

УДК 621.391

АНАЛИЗ ПУТЕЙ СНИЖЕНИЯ СЛОЖНОСТИ АЛГОРИТМОВ МЯГКОГО ДЕКОДИРОВАНИЯ ПОМЕХОУСТОЙЧИВЫХ КОДОВ

Все существующие методы декодирования помехоустойчивых кодов можно разделить на два класса: методы жесткого декодирования и методы мягкого декодирования. Применение оптимальных методов мягкого декодирования помехоустойчивых кодов позволяет снизить отношение сигнал/шум приблизительно на 2 дБ при сохранении заданной достоверности передачи информации по сравнению с методами жесткого декодирования. Недостатком оптимальных методов мягкого декодирования является большая сложность практической реализации, которая ограничивает сферу их применения [1 – 3].

Наиболее широко методы мягкого декодирования стали использоваться с появлением каскадных кодов, допускающих эффективное итеративное декодирование с обменом мягкими решениями на каждой итерации (турбокодов и аналогичных им каскадных кодовых конструкций на основе блочных кодов) [4].

Таким образом, актуальной задачей является разработка субоптимальных методов и алгоритмов мягкого декодирования помехоустойчивых кодов (как сверточных, так и блочных) уменьшенной сложности. Для решения такой задачи сначала необходимо с единых позиций провести анализ оптимальных методов мягкого декодирования помехоустойчивых кодов и обобщить подходы, направленные на уменьшение сложности алгоритмов мягкого декодирования.

Целью работы является проведение анализа оптимальных методов мягкого декодирования помехоустойчивых кодов и обобщение подходов, направленных на уменьшение сложности алгоритмов мягкого декодирования.

Математическая постановка задачи оптимального декодирования. Пусть $\overline{m}_i$ – i-е передаваемое сообщение (информационная последовательность) длиной K двоичных символов, $\overline{m}_i = (m_{i1}, m_{ij}, ..., m_{iK})$, $i = 1 ... 2^K$.

Пусть $\bar{x}_i$ – i-е кодовое слово блочного систематического помехоустойчивого (N, K) кода, $\bar{x}_i = (x_{i1}, x_{ij}, ..., x_{iK}, x_{iK+1}, ..., x_{iN})$, $i = 1 ... 2^K$ (кодовая последовательность). Если считать, что первые K символов кодового слова представляют собой передаваемое сообщение $\bar{m}_i = (x_{i1}, x_{i2}, ..., x_{iK})$, то справедливо равенство $\bar{x}_i = (\bar{m}_i, \bar{c}_i)$, где $\bar{c}_i$ – последовательность проверочных символов кода.

Будем считать, что заданы:

вероятности передачи сообщений (кодовых слов) $\Pr(\bar{m}_i) = \Pr(\bar{x}_i)$, $i = 1 ... 2^K$ или вероятности того, что символ x_j, $j = 1 ... N$ примет значение 1 и 0 – $\Pr(x_j = 0)$ и $\Pr(x_j = 1)$, причем $\Pr(x_j = 0) + \Pr(x_j = 1) = 1$;

условная плотность вероятности $p(\bar{y} / \bar{x}_i)$ принимаемой последовательности $\bar{y}$, $\bar{y} = (y_1, y_2, ..., y_K, y_{K+1}, ..., y_N)$ на входе декодера при условии, что передается кодовое слово $\bar{x}_i$. Отметим, что для канала без памяти справедливо равенство $p(\bar{y} / \bar{x}_i) = \prod_{j=1}^{N} p(y_i / x_{ij})$, где $p(y_i / x_{ij})$ – условная плотность вероятности принятого символа y_i при условии, что передан символ x_{ij}.

Задачу оптимального декодирования помехоустойчивого кода можно сформулировать двумя способами:

1. По принятой последовательности $\bar{y}$ вынести оптимальное по критерию минимума средней вероятности ошибки последовательности решение о том, какое именно сообщение $\bar{m}_i$ из множества возможных сообщений было передано [5].

2. По принятой последовательности $\bar{y}$ вынести оптимальное по критерию минимума средней вероятности ошибки символа решение о том, какое значение имеет символ x_j.

Далее рассмотрим оптимальные методы мягкого декодирования помехоустойчивых кодов с минимизацией средней вероятности ошибки последовательности и минимизацией средней вероятности ошибки символа.

Мягкое декодирование помехоустойчивых кодов с минимизацией средней вероятности ошибки последовательности. В этом случае оптимальным является решение, принимаемое по максимуму апостериорной вероятности последовательности:

$$\hat{\bar{m}} = \bar{m}_i,$$

если

$$\Pr(\bar{x}_i / \bar{y}) > \Pr(\bar{x}_j / \bar{y}) \quad \forall j \neq i, \; j = 1 ... 2^K. \tag{1}$$

Воспользуемся формулой Байеса для нахождения $\Pr(\bar{x}_i / \bar{y})$: $\Pr(\bar{x}_i / \bar{y}) p(\bar{y}) = p(\bar{y} / \bar{x}_i) \Pr(\bar{x}_i)$, откуда

$$\Pr(\bar{x}_i / \bar{y}) = p(\bar{y} / \bar{x}_i) \frac{\Pr(\bar{x}_i)}{p(\bar{y})}. \tag{2}$$

Плотность вероятности $p(\bar{y} / \bar{x}_i)$ будем рассматривать как функцию $\bar{x}_i$ при фиксированной реализации последовательности на входе декодера $\bar{y}$ и в дальнейшем называть функцией правдоподобия [5]. При равновероятных сообщениях оптимальным является решение, принимаемое по максимуму функции правдоподобия (так как $p(\bar{y})$ не зависит от $\bar{x}_i$), а декодер называется декодером максимального правдоподобия:

$$\hat{\bar{m}} = \bar{m}_i,$$

если

$$p(\bar{y} / \bar{x}_i) > p(\bar{y} / \bar{x}_j) \quad \forall j \neq i, \; j = 1 ... 2^K.$$

Мягкое декодирование помехоустойчивых кодов с минимизацией средней вероятности ошибки символа. Методы мягкого декодирования с посимвольным принятием решений являются базовыми при разработке итеративных методов декодирования помехоустойчивых кодов.

Как и в предыдущем случае, оптимальным есть решение, принимаемое по максимуму апостериорной вероятности, но не последовательности, а одного символа:

$$\hat{x}_j = 0, \text{ если } \Pr(x_j = 0 / \bar{y}) > \Pr(x_j = 1 / \bar{y});$$

$$\hat{x}_j = 1, \text{ если } \Pr(x_j = 1 / \bar{y}) > \Pr(x_j = 0 / \bar{y}),$$

где $\Pr(x_j = 0 / \bar{y})$ – апостериорная вероятность того, что символ $x_j = 0$;

$\Pr(x_j = 1 / \bar{y})$ – апостериорная вероятность того, что символ $x_j = 1$.

Аналогично выражению (2) можно записать:

$$\Pr(x_j = \alpha/\bar{y}) = p(\bar{y}/x_j = \alpha)\frac{\Pr(x_j = \alpha)}{p(\bar{y})}, \quad (3)$$

где $\alpha = 0,1$.

Теперь считая, что известны плотности вероятности $p(\bar{y}/\bar{x}_i)\ \ \forall i = 1 \ldots 2^K$, а также полагая значения всех символов, кроме x_j, несущественными, найдем $p(\bar{y}/x_j = \alpha)$, $\alpha = 0,1$ путем статистического усреднения $p(\bar{y}/\bar{x}_i)$ по несущественным символам:

$$p(\bar{y}/x_j = \alpha) = \sum_{\substack{\forall i = 1 \ldots 2^K, \\ \text{если } x_{ij} = \alpha}} p(\bar{y}/\bar{x}_i)\Pr(\bar{x}_i'),$$

где $\bar{x}_i = \{\bar{x}_i', x_{ij}\}$.

Используя (3), определим $\Pr(x_j = \alpha/\bar{y})$:

$$\Pr(x_j = \alpha/\bar{y}) = p(\bar{y}/x_j = \alpha)\frac{\Pr(x_j = \alpha)}{p(\bar{y})} =$$

$$= \frac{1}{p(\bar{y})}\Pr(x_j = \alpha) \sum_{\substack{\forall i = 1 \ldots 2^K, \\ \text{если } x_{ij} = \alpha}} p(\bar{y}/\bar{x}_i)\Pr(\bar{x}_i').$$

В полученном выражении внесем множитель $\Pr(x_j = \alpha)$ под знак суммы и, учитывая, что для независимых X_j – $\Pr(\bar{x}_i/\bar{y}) = \Pr(\{\bar{x}_i', x_{ij} = \alpha\}/\bar{y}) = \Pr(x_j = \alpha)\Pr(\bar{x}_i')$, получим:

$$\Pr(x_j = \alpha/\bar{y}) = \frac{1}{p(\bar{y})} \sum_{\substack{\forall i = 1 \ldots 2^K, \\ \text{если } x_{ij} = \alpha}} p(\bar{y}/\bar{x}_i)\Pr(\bar{x}_i). \quad (4)$$

Анализ выражений (1) и (4) показывает, что общим для двух оптимальных методов мягкого декодирования помехоустойчивых кодов является нахождение апостериорных вероятностей всех возможных кодовых последовательностей. А отличие состоит в том, каким образом найденные апостериорные вероятности используются для принятия решения.

Основные подходы, направленные на уменьшение сложности алгоритмов мягкого декодирования помехоустойчивых кодов. Рассмотренные выше оптимальные методы мягкого декодирования могут быть реализованы только для коротких кодов, так как сложность соответствующих алгоритмов декодирования пропорциональна количеству всех возможных кодовых слов, то есть $\sim 2^K$.

Кроме того, эти методы в явном виде не учитывают структуру кода (взаимосвязь информационных символов с проверочными) и требуют только знания образцов всех возможных кодовых последовательностей. Однако в общем случае учет особенностей структуры кода позволяет существенно снизить сложность алгоритмов мягкого декодирования. Поэтому далее обобщим основные подходы, направленные на уменьшение сложности алгоритмов мягкого декодирования помехоустойчивых кодов (как оптимальных, так и субоптимальных).

1. Представление помехоустойчивого кода с помощью графа. Такой подход позволяет представить кодовое слово как путь в графе, а декодирование рассматривать как поиск пути, соответствующего кодовому слову с наибольшим значением апостериорной вероятности.

Наиболее эффективным этот подход оказался для сверточных кодов, обладающих регулярной решетчатой структурой с постоянным числом состояний на каждом ярусе решетчатой диаграммы, не зависящим от длины информационной последовательности.

Примерами алгоритмов декодирования, использующих решетчатую диаграмму сверточных кодов, является алгоритм Витерби [6] и MAP-алгоритм [7].

Сложность таких алгоритмов определяется в основном числом состояний решетчатой диаграммы на одном ярусе – числом состояний кодера с памятью ν как 2^ν – и линейно зависит от длины информационной последовательности.

Применение данного подхода к блочным кодам наталкивается на определенные трудности, так как решетчатая диаграмма блочных кодов является в общем случае нерегулярной с числом состояний 2^{N-K}.

2. Использование множества проверочньх уравнений помехоустойчивого кода. Для помехоустойчивого (N, K) кода можно образовать 2^{N-K} проверочных уравнений путем линейной комбинации строк проверочной матрицы.

Такой подход применяется при мягком декодировании с минимизацией средней вероятности ошибки символа. В этом случае мягкое решение символа определяется совокупностью вкладов от всех возможных проверочных уравнений, в которые входит данный символ.

Примером использования такого подхода является алгоритм Хартмана − Рудольфа [3], рассматривающий 2^{N-K} линейных комбинаций строк проверочной матрицы как кодовые слова дуального кода. Сложность алгоритма Хартмана − Рудольфа определяется числом проверочных уравнений, которые используются для получения мягкого решения символа, то есть $\sim 2^{N-K}$.

Частным случаем метода Хартмана − Рудольфа можно считать методы порогового декодирования [1 − 3]. Они используют не все возможные проверочные уравнения, а только те, которые ортогональны по данному символу, недостатком которых является ограниченный класс кодов, к которым этот метод применим.

3. Порождение некоторого числа кодовых слов с большими значениями апостериорных вероятностей (порождение кодовых слов, наиболее близких к передаваемому кодовому слову).

Суть данного подхода заключается в аппроксимации правила (1) путем использования для сравнения только наиболее значимых членов, что позволяет существенно снизить сложность алгоритмов декодирования.

Порождение кодовых слов, наиболее близких к передаваемому кодовому слову, возможно, например, если считать, что ошибки содержатся только на позициях наименее достоверных символов.

Среди методов, использующих этот подход, можно выделить методы перестановочного декодирования [3], метод декодирования по обобщенному минимальному расстоянию [2] и методы Чейза [3].

Таким образом, была показана взаимосвязь оптимальных методов мягкого декодирования помехоустойчивых кодов с минимизацией средней вероятности ошибки последовательности и минимизацией средней вероятности ошибки символа. Обобщены подходы, направленные на уменьшение сложности алгоритмов мягкого декодирования помехоустойчивых кодов.

Литература: 1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Под ред. К. Ш. Зигангирова. – М.: Мир, 1986. – 576 с. 2. Витерби А. Д. Принципы цифровой связи и кодирования: Пер. с англ. / А. Д. Витерби, Дж. К. Омура; [Под ред. К. Ш. Зигангирова. – М.: Радио и связь, 1982. – 536 с. 3. Кларк Дж.-мл. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Кларк Дж.-мл., Кейн Дж.; [Под ред. Б. С. Цыбакова. – М.: Радио и связь, 1987. – 392 с. 4. Berrou C., Glavieux A., Thitiumjshima P. Near Shannon limit error correcting coding: Turbo codes // Int. Conf. on Commun. – Geneva, Switzerland. 1993. – P. 1061 – 1070. 5. Долгов В. И. Основы статистической теории приема дискретных сигналов. – Харьков: ХВВКИУ РВ, 1989. – 448 с. 6. Витерби А. Границы ошибок для сверточных кодов и асимптотически оптимальный алгоритм декодирования // Некоторые вопросы теории кодирования. – М., 1970. – С. 142 – 165. Pietrobon S S., Barbulescu A.S. A simplification of the modified Bahl decoding algorithm for systematic convolutional codes // Int. Symp. on Inform. Theory and its Applications. – Sydney, Australia. – November 1994 – P. 1073 – 1077.

Секція 3
Інформаційні та телекомунікаційні системи в бізнесі

Горбань В. Б.

УДК 681.518:621

ФОРМУВАННЯ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ШЛЯХИ ЇЇ АДАПТАЦІЇ ДО ДІЯЛЬНОСТІ МАШИНОБУДІВНИХ ПІДПРИЄМСТВ

З метою підвищення якості внутрішнього управління, ефективності й конкурентоспроможності, гнучкості та стійкості до зовнішніх впливів і, як наслідок, досягнення прибуткової діяльності машинобудівні підприємства потребують щоразу нових підходів щодо організації своєї діяльності. На сьогодні надзвичайно актуальним залишається питання побудови ефективної інформаційної системи підприємств машинобудівного комплексу.

Корпоративна інформаційна система (КІС) – це комплекс програм, або програмна система, яка забезпечує реалізацію основних бізнес-процесів підприємства [1, с. 2].

У минулому замість терміна КІС широко застосовувався термін АСУП (автоматизована система управління підприємством). Однак трансформаційні процеси в економіці наклали свій відбиток на термін АСУП, дискредитувавши його [2, с. 1 – 2].

КІС – надзвичайно важлива для підприємства, адже наслідком її впровадження є збільшення обсягів продажу продукції підприємства, зниження її собівартості, зменшення величини складських запасів, скорочення термінів виконання замовлень, покращання договірних відносин з постачальниками та ін.

Однак, незважаючи на перелічені вище переваги, питання окупності інвестицій у КІС не втрачає своєї актуальності. Співвідношення переваг від використання системи і її вартості є одним із найважливіших факторів, які мають вирішальний вплив на процес прийняття рішення щодо купівлі КІС та її впровадження.

Упровадження КІС, безумовно, можна розглядати як інвестиційний проект, а тому актуальними є питання оцінки його вартості та очікуваної окупності. Безпосередню окупність КІС підрахувати досить важко, адже в результаті її впровадження оптимізується внутрішня структура підприємства, знижуються його транзакційні витрати. Вкрай нелегко оцінити ефект від ліквідації хаосу, адже важко визначити, який розмір витрат несе підприємство внаслідок збою термінів виконання замовлень, неточностей в асортименті; який обсяг ресурсів є виведеним з обороту внаслідок відмінностей в обліку даних у бухгалтерії і на складах; і яким чином оцінити обсяг крадіжок та розбазарювання ресурсів.

Проте в деяких аспектах діяльності підприємства оцінка ефективності КІС є цілком реальною. У першу чергу, це стосується логістики, де впровадження КІС призводить до оптимізації матеріальних потоків і до зниження потреби в обігових коштах. Побудова на базі КІС системи фінансового контролінгу призводить до зниження накладних витрат підприємства, ліквідації збиткових підрозділів та виключення з асортименту нерентабельної продукції чи послуг.

За даними незалежних інформаційних агентств, при правильному, ретельно спланованому впровадженні КІС підприємства можуть досягнути дійсно значних результатів, а саме: зниження транспортно-заготівельних витрат – на 60%; скорочення виробничого циклу з виробництва продукції на замовлення – на 50%; скорочення кількості затримок із відвантаження готової продукції – на 45%; зменшення рівня залишків продукції на складах – на 40%; зниження виробничого браку – на 35%; зменшення адміністративно-управлінських витрат – на 30%; скорочення виробничого циклу з виробництва основної продукції – на 30%; зменшення складських площ – на 25%; зменшення дебіторської заборгованості – на 12%; зниження страхового рівня складських запасів – на 12%; збільшення обігових коштів у розрахунках – на 30%; збільшення оборотності товарно-матеріальних цінностей – на 65%; збільшення кількості поставок "точно в строк" – на 80% [1, с. 4].

Мету статті автор вбачає у доцільності розробки методики формування КІС підприємства та дослідження можливостей її впровадження у діяльність підприємств машинобудівного комплексу.

Для успішного розвитку підприємства необхідні дві умови: наявність конкурентних переваг і ефективна організація системи управління. Система управління повинна максимально швидко реагувати на зміни зовнішнього та внутрішнього середовища і здійснювати керівництво над шляхом досягнення цільових показників. Для системи управління інформаційна система є настільки важливою, як нервова система для людини. КІС – це підсистема системи управління, а тому вона здійснює підтримку повного циклу управління: планування, організації, мотивації, контролю та регулювання [3, с. 4].

На сьогодні існує безліч підходів щодо формування КІС. Її різновидність залежить від компанії, що її розробляє, і від її бачення очікуваних результатів, яких можна досягти при впровадженні КІС. Традиційні підходи побудови КІС ґрунтуються на тому, що на початку проекту важко передбачити, які дані повинні міститися в базі даних і які аналітичні завдання мають вирішуватись кінцевими користувачами.

На сьогодні надзвичайно поширеним є підхід RAD (Rapid Application Development – швидка розробка додатків), який зарекомендував себе при створенні невеликих додаткових функціональних систем [4, с. 1 – 2].

Однак для машинобудівних підприємств цей підхід є недосконалим, адже створення КІС машинобудівного підприємства вимагає реінжинірингу бізнес-процесів, а саме бізнес-інжинірингу, тобто створення організації, орієнтованої на реалізацію конкретно визначеної стратегії. Саме тому для машинобудівних підприємств найбільш перспективно використовувати бізнес-орієнтований підхід, заснований на BSC (Balanced Scorecard – система збалансованих показників). Він дає можливість прогнозувати зміни в бізнесі та сформувати цілісну картину розвитку підприємства як мінімум за чотирма напрямками – фінансовим, маркетинговим, організаційно-технологічним та напрямком інновацій [4, с. 2].

За доцільне вважаємо систематизувати підходи впровадження КІС та запропонувати авторське бачення методики її впровадження у діяльність підприємств, у тому числі і підприємств машинобудівного комплексу.

Таким чином, можна виділити сім основних етапів управління проектом побудови КІС на підприємстві.

Першим етапом є **усвідомлення потреби в автоматизації**. Це концептуальний етап, однак без нього неможлива подальша реалізація проекту.

Другий етап полягає у **проектуванні "карти стратегії" впровадження КІС.**

"Карта стратегії" впровадження КІС – це її графічне відображення у вигляді набору причинно-наслідкових зв'язків. Для кожної перспективи (фінанси, маркетинг, технології, інновації) повинні бути визначені стратегічні цілі і здійснена побудова дерева цілей.

Третій етап передбачає **визначення цілей упровадження КІС та розбиття їх на конкретні завдання.**

Він реалізується через наступні заходи:

проведення бенчмаркетингу: аналіз досвіду інших підприємств близького профілю діяльності та галузевої приналежності;

визначення цілей проекту в контексті підвищення ефективності вирішення існуючих управлінських завдань і можливостей упровадження нових управлінських рішень;

визначення узагальнених показників ефективності бізнес-процесів, які підлягають автоматизації, та формування першочергових критеріїв успішності проекту.

Четвертий етап передбачає проведення **обстеження підприємства і підготовку проекту до впровадження.** Реалізацію цього етапу доцільно здійснювати в наступній послідовності:

1. Вибір консалтингової компанії для проведення комплексного обстеження і формування технічних завдань для автоматизації або проведення обстеження власними силами.

2. Вибір різновиду КІС, що підлягає впровадженню.

На сьогодні існує безліч різновидів КІС, які можна запропонувати для впровадження у діяльність підприємств, а саме: MPS (Master Planning Schedule) – методологія "об'ємно-календарного планування"; MRP (Metrical Requirements Planning) – методологія планування потреби в матеріальних ресурсах; CRP (Capacity Requirements Planning) – планування виробничих ресурсів; FRP (Finance Requirements Planning) – планування фінансових ресурсів; MRPII (Metrical Resources Planning) – планування виробництва; ERP (Enterprise Resources Planning) – концепція бізнес-планування; CSRP (Customer Synchronized Resources Planning) – планування ресурсів, синхронізованих з покупцем; SCM (Supply Chain Management) – управління ланцюгом постачання; CRM (Customer Relationship Management) – концепція побудови автоматизованих систем обслуговування клієнтів підприємств та ін.

Головним критерієм, яким має керуватись підприємство, є плановий очікуваний результат, якого воно бажає досягти, і які сфери діяльності бажає покращити [1, с. 4 – 5].

Для машинобудівних підприємств, які здійснюють випуск унікальної продукції високої вартості, надзвичайно важливим є те, щоб КІС мала високорозвинену підсистему логістики, потужні засоби проектного управління та виробничого планування.

3. Вибір компанії, яка буде здійснювати впровадження (з можливістю організації тендеру).

При аналізі претендентів слід керуватись наступними факторами: наявність формалізованої методології проектного управління, висока ділова репутація компанії, присутність кваліфікованих консультантів та бізнес-аналітиків, позитивний досвід роботи в аналогічних проектах.

4. Підготовка персоналу підприємства до проекту змін та розробка нової політики мотивації праці.

5. Затвердження проектної методології шляхом формування моделі команди, моделі процесів та моделі можливих ризиків.

Модель команди визначає розподіл ролей у межах робочих груп, правила їх взаємодії та відповідальність за виконання проектних завдань. Модель процесів описує регламент виконання робіт, звітну політику і правила представлення результатів протягом життєвого циклу проекту. Модель ризиків описує правила виявлення ризиків, а також принципи пошуку шляхів їх усунення чи зниження їх рівня [5, с. 10].

6. Вибір критеріїв успішності проекту побудови КІС.

7. Управління проектом організаційних змін.

8. Розробка та затвердження графіка досліджень, а також функціональних і технічних вимог до ПК.

П'ятим етапом упровадження КІС є **вибір постачальника ПК та укладання контракту щодо технічного переоснащення підприємства**, який передбачає: формування вимог до ПК та до постачальників ПК; вибір компанії, що буде здійснювати технічне переоснащення (з можливістю організації тендеру); вибір форми співробітництва і підписання контракту з постачальниками ПК [1, с. 11].

Шостий етап полягає у забезпеченні **управління проектом побудови й розвитку КІС**. Він реалізується через наступні заходи:

1) управління моделями робочої групи проектів, виробничих процесів та можливих ризиків;

2) управління конфігурацією ПК, тестуванням та стабілізацією;

3) управління ризиками і якістю впровадження;

4) розробка правил роботи з КІС та затвердження процедури внесення змін у конфігурації;

5) навчання і сертифікація користувачів та адміністраторів;

6) організація роботи підрозділів технічної підтримки.

Заключним етапом є **апробація проекту впровадження КІС**.

Однак зауважимо, що процес управління проектом розвитку КІС нескінченний: його динаміка визначається темпом змін усіх складових елементів системи і, в першу чергу, розвитком бізнесу підприємства.

Успішне впровадження корпоративної інформаційної системи приведе до позитивних змін у діяльності машинобудівних підприємств і появи нових можливостей їх розвитку, а саме: вплине на здатність передбачити й задовольнити весь спектр потреб з обслуговування клієнтів, забезпечить підтримку нарощування капіталу і розвитку трудових ресурсів, дасть можливість адекватно оцінити масштаби ринків збуту продукції та своєчасно реагувати на зміни законодавства, забезпечить оперативну реакцію на зміни потреб ринку.

У перспективі доцільним вважаємо дослідження процесу впровадження КІС у діяльність машинобудівних підприємств в аспекті покращання їх мотиваційної політики.

Література: 1. Баранов В. Двадцать один вопрос о корпоративных информационных системах // www. iteams. ru/publications /it/section_52/ article_2210/ 2. Богач А. Розвиток інформаційних систем промислових підприємств на принципах аналітико-логістичної системи інформації // Наукові записки. – 2006. – Вип. 15. – С. 64 – 66. 3. Сысовская Е. Место информационной системы в системе управления // www. iteams.ru /publications/it/section_52/ article_2010/ 4. Галахов И. Проектирование корпоративной информационно-аналитической системы // Открытые системы. – 2003. – №4. – С. 25 – 33. 5. Верников Г. Корпоративные информационные системы: не повторяйте пройденных ошибок //www. iteams. ru/publications /it/section_52/ article_109/

Беседовський О. М.

Гаврилова А. А.

УДК 331.108.36:051-023

СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЗВІТУВАННЯ ПЛАТНИКІВ ПОДАТКІВ В УКРАЇНІ ТА ХАРКІВСЬКІЙ ОБЛАСТІ

Формування реєстру податкових накладних, відстеження сум проплат та зустрічі з перевірниками, постійний збір необхідної інформації, з одного боку, та вихід на підприємства, написання актів, з іншого – на сьогодні притаманні системі відшкодування сум податку на додану вартість (ПДВ) та вимагають затрат часу як самого платника, так і працівників податкових органів. З метою підвищення якості обслуговування платників податків при наданні ними податкової звітності, зменшення документообігу, мінімізації втручання в господарську діяльність суб'єктів підприємницької діяльності Державна податкова адміністрація (ДПА) України розробила та впровадила систему прийому податкової звітності в електронному вигляді засобами E-mail із застосуванням електронного ключа та електронного цифрового підпису задля забезпечення повної конфіденційності інформації, яка передається.

Тому дана робота присвячена розгляду й аналізу переваг автоматизованої інформаційної системи контролю завдання податкової звітності як для платників податків, так і для Державної податкової служби України.

Донедавна податкова звітність надавалася комбінованим способом, тобто одночасно з файлом на магнітному носії здавалася форма декларації, роздрукована на паперовому носії. Для таких клієнтів у залах прийому звітів у податкових інспекціях виділялися окремі "вікна" і вони обслуговувалися "без черги". Сьогодні ДПА України, виконуючи численні побажання бухгалтерів, удосконалила систему здавання податкової звітності – тепер можна звітувати не тільки "без черги", але й не виходячи з офісу. Із червня 2006 р. у всіх податкових інспекціях уведена в експлуатацію система прийому податкової звітності й податкових накладних в електронному вигляді, що дозволила почати прийом звітності через Internet [1]. Дана система успішно функціонує на території України й одержала ряд позитивних відгуків від суб'єктів господарювання, що підключилися до неї.

Програмою розвитку ДПА України передбачене створення партнерських взаємин із платниками податків з метою збільшення надходжень від добровільної сплати податків і поліпшення якості обслуговування суб'єктів підприємницької діяльності. Розвиток цифрових технологій та створення нормативно-правової бази, що регулює електронний документообіг відповідно до європейських стандартів, дозволило надавати звітність в електронному вигляді. Будь-яке підприємство, що має комп'ютер, підключений до глобальної мережі Internet, може пересилати податкову звітність на електронну поштову скриньку податкової інспекції через E-mail. Це стало можливим після прийняття відповідних законів і затвердження міжнародного формату (стандарту) електронного документа на підставі специфікації eXtensible Markup Language (XML) [2; 3].

Автоматизована системи звітування має значні переваги перед існуючою системою подання звітності, бо дозволяє спрощувати процедури подання податкової звітності платника податків до органів ДПС, зменшувати паперовий документообіг, приводити до єдиних стандартів документообігу в органах ДПС і у платників податків щодо ведення обліку податкової звітності та реєстрів отриманих і виданих податкових накладних, автоматизувати обробку та аналіз реєстрів отриманих і виданих податкових накладних в єдиній базі даних за умов обмеження та контролю доступу до показників платників податків, що не дасть можливості зловживання протизаконними схемами відшкодування коштів ПДВ з державного бюджету, спрощувати процедури підтвердження сум до відшкодування, зменшувати терміни проведення перевірок, своєчасно відшкодовувати податок на додану вартість при обмеженому спілкуванні з представниками органів фінансового контролю та скасовувати необґрунтовані виїзні перевірки платників податків [4].

Згідно зі статистичними даними ДПА України [4], станом на 01.01.2008 р. розподіл регіонів України за кількістю платників податків, які звітують в електронній формі та за допомогою паперових носіїв, наведено на рис. 1. У діаграмі більш детально було відображено інформацію за тими регіонами, в яких кількість платників податків, що використовують безпаперові технології звітування, перевищує 1 тис. платників. Але питома вага платників податків регіонів-лідерів з електронного звітування залишається дуже малою порівняно з тим, скільки платників користуються технологією паперового подання податкових звітів. До регіонів, у яких найбільш популярна система подання звітності в електронному вигляді, належить чотири області України – Київська (32 697 платників), Дніпропетровська (15 332 платника), Донецька (15 037 платників) та Харківська (11 492 платника).

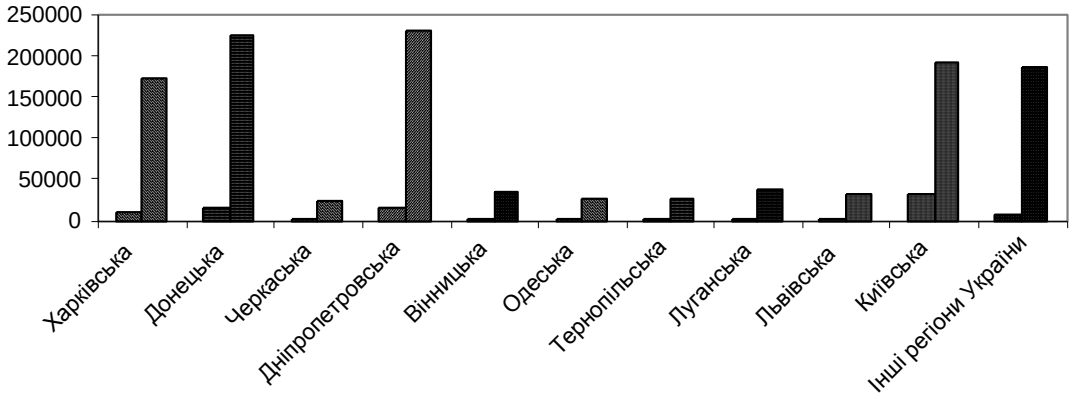


Рис. 1. **Стан використання технологій звітування платників податків в органи оподаткування за регіонами України на 01.01.2008 р.**

Стосовно способів електронного звітування, то їх існує два: за допомогою магнітних носіїв інформації (на дискеті чи лазерному диску) (рис. 2) та за допомогою засобів телекомунікаційного зв'язку (Internet) (рис. 3).

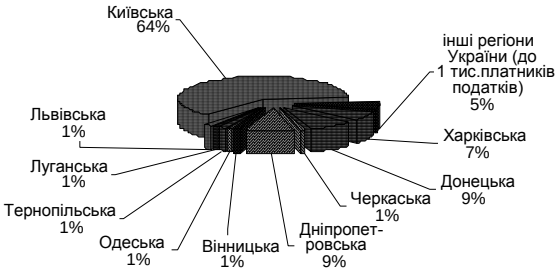


Рис. 2. **Розподіл регіонів України за кількістю платників податків, які звітують в електронній формі за допомогою магнітних носіїв інформації**

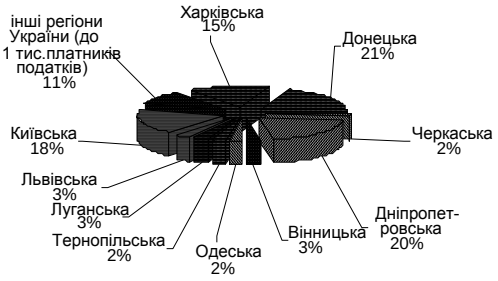


Рис. 3. **Розподіл регіонів України за кількістю платників податків, які звітують в електронній формі за допомогою засобів телекомунікаційного зв'язку**

Лідерами з використання засобів Internet на 01.01.2008 р. є Донецька (21%) та Дніпропетровська (20%) області (див. рис. 3). Також дуже високі показники в Київському (18%) та Харківському (15%) регіонах, але слід зазначити, що платники податків м. Київ та Київської області все ж таки значну перевагу ще віддають технології передачі інформації на магнітних носіях, що говорить про високий рівень недовіри до захисту конфіденційної інформації при застосуванні телекомунікаційного зв'язку (див. рис. 2). Вінницька, Черкаська, Одеська, Тернопільська, Луганська та Львівська області характеризуються приблизно однаковим рівнем застосування двох вищезазначених технологій передачі звітності електронним способом (див. рис. 2, рис. 3).

Стосовно Харківського регіону, спираючись на статистичні дані ДПІ м. Харкова та Харківської області, можна зробити висновок про те, що станом на 01.01.2008 р. з 40 258 юридичних осіб, які є платниками податків, тільки 21,5% використовують можливість пересилання податкової звітності в ДПІ за допомогою засобів Internet, для фізичних осіб ця частка дорівнює лише 2% із 142 152 платників податків [5].

Але, незважаючи на те, що дані цифри далекі від бажаних, навіть у цієї частини платників податків є можливість вибору того програмного комплексу для формування й передачі електронної податкової звітності, що найбільше їх влаштовує.

Донедавна документ у форматі XML можна було створювати, якщо були встановлені такі програмні комплекси, як "Бест-Звіт плюс", "1С", "Ліга-Закон" або будь-які інші самостійно написані програми. Це доставляло ряд незручностей, пов'язаних, наприклад, з тим, що при формуванні звіту в "1С" і збереженні його в XML-форматі часто доводилося за деякими формами корегувати XML-файли вручну, щоб вони нормально імпортувалися в податковій інспекції. Ще необхідно зазначити, що, перш ніж формувати податкову звітність даними програмними засобами, спочатку потрібно зробити наступне: або придбати ці засоби ("1С"), або щомісяця мати експлуатаційні витрати, пов'язані з правом користування ними ("Бест-Звіт плюс" – 200 грн., "Ліга-Закон" – 400 грн.), або проводити трудомісткі роботи зі створення своїх технологій.

Тому ДПА України, прислухаючись до побажань платників податків і використовуючи міжнародний досвід, розробила й розіслала по областях програмне забезпечення, що призначене для формування й обробки податкових декларацій, податкових накладних і реєстру отриманих, виданих податкових накладних в електронному вигляді, для безкоштовного поширення серед платників податків. Це програмне забезпечення не має функцій бухгалтерського обліку, але є інструментом для заповнення бланка звітності в його електронному представленні, що дозволяє зберегти дані в XML-форматі. З цієї ж програми звіт можна видрукувати, тобто не потрібно купувати бланки. Програмне забезпечення для накладання цифрового підпису також безкоштовне. Електронна звітність не потребує майже нічого, що могло б ускладнити роботу бухгалтера чи податкового інспектора. Тут немає ні паперів, ані громіздких архівів, ані біганини й очікування в чергах. Окрім того, відсутній безпосередній контакт платника з податківцем, а отже, і підґрунтя для багатьох негативних явищ.

На сьогодні для зазначених цілей пропонується програмне забезпечення "Нотар", яке використовується в системі подання електронної податкової звітності до органів ДПС України і призначене для накладення електронного цифрового підпису (ЕПЦ) на електронний документ належного формату. Використання даного підходу дозволяє вирішувати проблему захисту конфіденційної інформації при передачі її електронними каналами зв'язку. Успішність цього рішення пов'язана із застосуванням системи криптографії, з відкритим та закритим ключами, пов'язаними між собою унікальними математичними перетвореннями, які на теперішній час не мають рішення. Це означає, що закритий ключ, за допомогою якого розшифровується відправлена інформація, неможливо підібрати. Тому програмне забезпечення "Нотар" виконує наступні функції: генерація особистих ключових елементів платника податків (закриті та відкриті ключі керівника і бухгалтера); формування електронного носія з відкритими ключами платника податків для подання його в податкову інспекцію; накладання ЕПЦ на електронний документ податкової звітності та його шифрування; розшифровування електронної відповіді про результат прийому електронної звітності, отриманої від органу ДПС.

У результаті проведеного аналізу стану впровадження та використання автоматизованої системи звітування можна зробити висновки про те, що, незважаючи на ще малий обсяг тих, хто ви-

користовує дану технологію, вона з часом стане все ж таки найбільш прийнятною для вітчизняних платників податків, бо несе однаково вигідні риси не тільки для податківців та державного бюджету, а й для самих платників податків.

Так, очікувані результати від впровадження системи для платників наступні: зменшення паперового документообігу, спрощення процедури подання звітності до органів ДПС, спрощення процедури підтвердження сум до відшкодування, зменшення термінів проведення перевірок, своєчасність відшкодування ПДВ.

Для ДПС України очікувані результати при впровадженні системи наступні: автоматизований контроль за повнотою і своєчасністю надходження коштів для відшкодування, додатковий ефективний інструмент щодо адміністрування ПДВ, скорочення терміну проведення податкових перевірок щодо правочинності відшкодування заявлених сум ПДВ, зменшення витрат та робочого часу на проведення документальних і зустрічних перевірок, автоматизація відбору платників податків для проведення перевірок, підвищення рівня обслуговування платників податків.

Для державного бюджету України очікувані результати – це підвищення рівня збору, що дасть можливість у перспективі знизити податкове навантаження, оперативне підтвердження заявлених до відшкодування сум ПДВ, ліквідація заборгованості з відшкодування ПДВ, залучення до сплати потенційних платників та виведення з "тіні" тих платників, що ухиляються від оподаткування, ліквідація схем мінімізації податкових зобов'язань, "фіктивних" фірм.

Література: 1. Письмо ГНА Украины от 14.06.2006 г. №11253/7/28-6017 // www. liga. ua. 2. Закон України "Про електронні документи та електронний документообіг" від 22.05.2003 р. №851-IV та №852-IV // www. liga. ua. 3. Закон України "Про електронний цифровий підпис" від 03.05.2006 р. №242 // www. liga. ua. 4. www. sta. gov. ua 5. www. dpa. khakov. ua

УДК 642.12

Khodyrevskaya A. V.

THE IMMEASURABILITY PROBLEM OF IT INVESTMENT

The IT department typically has a large and rapidly growing budget. In addition, most IT departments have had at least a few high-profile failures, causing business executives to be somewhat suspicious of IT's value. If the line works, and IT leaders persuade business executives that IT investments are somehow fundamentally different from other types of business investment, IT is relieved of the responsibility of attaching dollar values to those investments.

Measuring methods of information technology investment is a part of business-performance management. It is rather young branch of knowledge, so the question of its effectiveness measurement is not comprehensively studied yet. The works of the following authors are devoted to the topic explored: Dr. Robert Kaplan, David Norton (the Balanced Scorecard) [1], Marilyn Parker, Robert Benson (Information Economics) [2], Ted Smith, Fernando Flores, Dale Skeen, Ismael Ghalimi, Phil Gilbert (Business-performance management) [3].

The first problem is that results have no meaning when compared to other investments. The second problem is that, to date, there is no empirical evidence that this method improves decisions.

The "immeasurability" problem is caused by three basic types of misunderstanding about measurement problems. Firstly, the object of measurement (i. e., the thing being measured) & the concept (the meaning) of measurement is not understood. The methods of measurement (proven techniques used by science) generally are not well understood [2].

The aim of this article is to define the IT investment effectiveness measuring problem field and to analyze business-performance management optimization methods.

Business-performance management, though defined in various ways, is generally considered to be a set of management and analytic processes – supported by technology – that addresses financial and operational activities.

Businesses set strategic goals and then measure and manage performance against those goals. Core processes include strategic, financial, and operational planning; consolidation and reporting; modeling and analysis; metrics such as scorecards and Six Sigma; and monitoring of key performance indicators linked to organizational strategy using dashboards.

Enterprises are using business-performance management for a variety of reasons. Among the common drivers: to improve decision making, reduce costs, increase accountability, improve business planning, and achieve better visibility into business processes such as sales.

As part of their efforts, companies are using various performance metrics and standards. The most popular are business-activity monitoring (61%), ISO 9000X (47%), balanced scorecards (44%), and Six Sigma (35%) [4].

One of the concepts in the Balanced Scorecard methodology that appeals to many executives or other business decision-makers is the idea of having "leading measures."

When Dr. Robert Kaplan and David Norton introduced the Balanced Scorecard over a decade ago, part of the "balance" that they introduced was balancing the traditional financial measure, which they characterized as lagging measures, with measures that gave a better indication of likely future performance-leading measures [1].

The Balanced Scorecard methodology stresses that objectives and measures from multiple perspectives should all be considered.

The classic perspectives for for-profit businesses are Financial, Customer, Internal Operations/Processes, and Learning and Growth (which focuses on human capital, technology and organizational culture − the intangible assets that create value).

By looking carefully at all four perspectives, organizations can focus on both the causal drivers of performance and the outcomes.

In the Balanced Scorecard, the strategic objectives often consist of a verb-adjective-noun phrase. For example, an objective may be something like "Grow International Sales" or "Build Deep Client Partnerships".

These objectives should be linked in cause and effect chains that cross the multiple scorecard perspectives — graphically depicted in what has become known as a strategy map.

The following diagram (fig. 1) shows objectives linked in cause and effect chains that are part of a strategy map for a software company based in the U. S. that wants to execute a strategy of growing international sales [1].

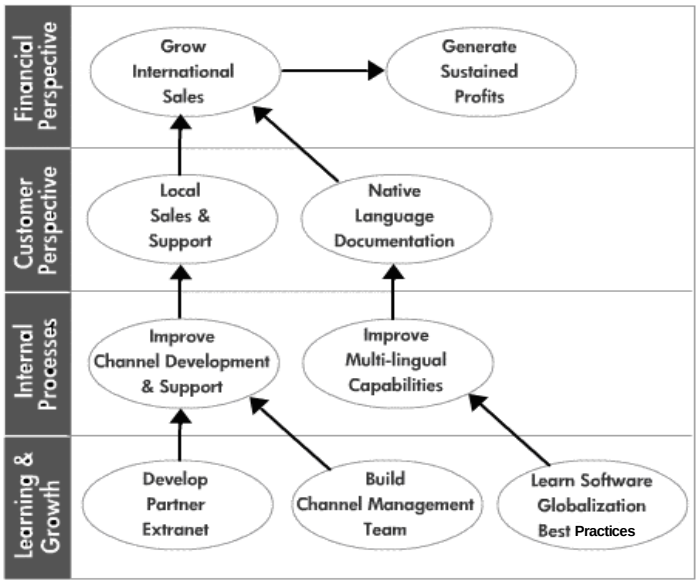


Fig. 1. **Part of a Strategy Map for a Software Company**

The graphical representation of KPIs and metrics (fig. 2) makes it easier to analyze the information in an efficient manner.

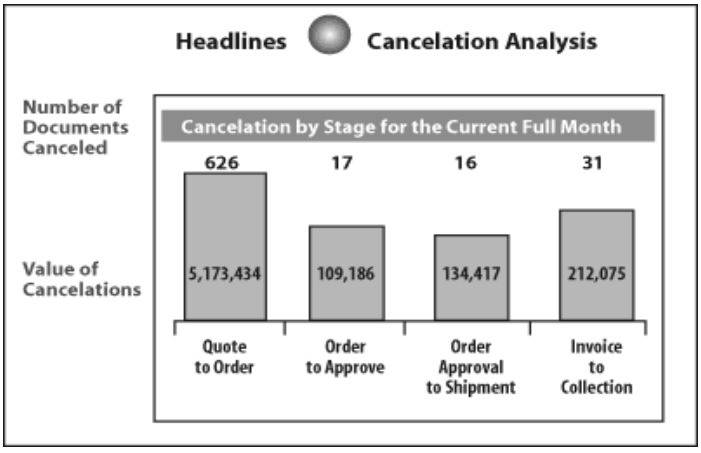


Fig. 2. **Detailed Metrics that Visually Represent Order Cancellation by Sales Process Stage**

Although selection of the appropriate visuals and graphs contribute to the effectiveness of a Business-performance management dashboard, the true "soul" of the dashboard is the key performance indicators (KPIs). They also provide the focal point for enterprise-wide standardization, collaboration and coordination.

Incorporating visualization with KPIs provides individuals with a powerful tool to manage the activities of their organization. Through visualization of KPIs, individuals can quickly and easily spot events or trends that are of concern and can focus their resources on those activities that require their attention.

There are several products categories that support visualization of KPIs. These product categories have their advantages and disadvantages where are highlighted in the table below (table) [4].

Table

Product categories that support visualization of KPIs

Product Category	Advantages	Disadvantages
Spreadsheet Software	1. Software is the least expensive of the three product categories. 2. Easy to use. 3. Rich in functionality	1. Manually intensive and prone to errors and inconsistencies. 2. KPIs and metrics will need to be defined. 3. Updates are time-consuming
Business Intelligence Software	1. Easy to use. 2. Rich in functionality. 3. Enables research and analysis through ad hoc query capabilities	1. Requires configuration of the software. 2. KPIs and metrics will need to be defined. 3. Presentation of the information may be too detailed and not in a manner that is suitable for executive or senior management
Analytic Applications	1. Easy to use. 2. Standard templates which contain KPIs and metrics by subject area are often available by vendor. 3. Automated process of data extraction and updating of KPIs and metrics	1. Software is the most expensive of the three product categories. 2. Requires configuration of the application and validation of KPIs and metrics. 3. No value is provided if the source data is not available for the subject area templates

Non-IT executives agree most strongly that the role of information technology in their organization is to reduce costs. Most agree that IT supports the needs of the company well, is an important part of the business and is aligned to company strategy. Less agreement can be found, however, for the statement that information technology represents a means to increase sales and/or to achieve competitive advantage.

There is a low level of agreement among non-IT executives that IT is a core competency of their organization. Surprisingly, most IT executives agree that information technology is a core competency of their company.

This increased conservatism is illustrated in the shortening of expected pay-back periods for information technology projects. Two-thirds of GMA-member companies (Grocery Manufacturers of America) expect IT projects to recoup their costs in one to two years – up from 43 percent last year. The numbers of those expecting a longer pay back of two to five years [5].

In order to effectively make informed business decisions, individuals must have access to relevant information. KPIs and metrics aid individuals with assessing performance, identifying activities or events that are of concern and focusing resources on those activities that require attention.

In this rapidly changing and competitive business environment, management needs all the relevant information that they can get to steer the best course for their organization.

To ensure that business-performance management works, companies evaluate their efforts fairly frequently. Despite the benefits, deployment can present significant challenges. Nearly three-quarters of those implementing business-performance management said they've had difficulty changing or adapting their corporate business processes to use it. About two-thirds have grappled with technical-integration issues in linking Business-performance management technologies with existing financial systems, and half have had a hard time educating IT and corporate employees about Business-performance management [6].

As a result of these and other efforts, such as standards, companies should achieve improvements not only in performance, but in their ability to measure their progress.

References: 1. Barberg Bill. Balanced Scorecard Best Practices: Understanding Leading Measures // ITNetwork365. – http://www. businessintelligence com/. 2. Hubbard Douglas. Everything Is Measurable // CIO. May, 2007. – http://www. cio. com/article/print/112101. 3. Silver Bruce. BPM Hall of Fame // BPMS Watch. March 22, 2008. – http://www. brsilver. com/wordpress/2008/03/22/bpm-hall-of-fame/ 4. Computer Sciences Corporation. 2003 Information Technology Investment Study. – http://www. gmaonline. org/publications/docs/03ITInvestmentStudy. pdf 5. Wu Jonathan. Visualization of Key Performance Indicators // DM Review Online. May 24, 2002. – http://www. dmreview. com/news/5229-1.html 6. Violino Bob. Getting Better All The Time // Information week. May, 2004. – http://www. informationweek. com/.

Бурдаев В. П.

УДК 004:33 (075.8)

ПОСТРОЕНИЕ БАЗ ЗНАНИЙ ДЛЯ ПРИНЯТИЯ БИЗНЕС-РЕШЕНИЙ

Современная конкуренция на различных рынках становится актуальной проблемой для решения нестандартных, творческих, креативных задач бизнеса.

Принятие решения в экономических системах связано с анализом большого объема разнородной, неполной и противоречивой информации и основывается на построении экономико-математических моделей. Для реализации таких моделей используют различные компьютерные системы принятия решения, например, экспертные системы, прецедентные экспертные системы.

Современная тенденция в сфере создания экспертных систем в экономике указала следующие направления их применения:

производство;
сбыт;
финансирование;
управление производством и персоналом;
логистика;
закупки;
запасы;
инвестиции, ценные бумаги.

Экспертная система (ЭС) – это компьютерная система, позволяющая на основе базы знаний, составленную экспертами из конкретной предметной области, с помощью логического вывода решить поставленную задачу. Такие системы еще называют системами, основанными на знаниях. Первые ЭС были созданы в 1980-х годах – это система "MYCIN" (диагностика бактериальных инфекций крови) и система "PROSPECTOR" (предметная область – геология) [1].

Основные компоненты ЭС: база знаний; база фактов; редактор базы знаний; машина логического вывода; подсистема объяснения; интерфейс пользователя и инженера знаний.

Эксперт – это высококвалифицированный специалист предметной области.

Инженер по знаниям (когнитолог) – это высококвалифицированный специалист по ЭС, осуществляющий извлечение знаний из эксперта и формализующий эти знания в соответствии с концептуальной моделью предметной области.

Пользователь – это специалист предметной области.

База знаний (БЗ) является совокупностью формализованных знаний о предметной области.

База фактов (БФ) представляет собой данные о процессах и явлениях предметной области.

Редактор БЗ позволяет вводить и корректировать формализованные знания.

Машина логического вывода представляет собой код программы, реализующий логический вывод на основе знаний БЗ.

Подсистема объяснения – это код программы, позволяющий выполнить трассировку логического вывода по применению знаний из БЗ.

ЭС создается в результате работы эксперта и инженера по знаниям на базе инструментальных средств систем искусственного интеллекта. Наиболее популярны для построения ЭС – это оболочки для создания ЭС, то есть компьютерные системы, содержащие те же компоненты, что и ЭС, но вместо БЗ используется только каркас БЗ, который следует заполнить знаниями соответствующей предметной области. Первая такая система получила название "EMYCIN", то есть префикс E (empty) означает, что ЭС "MYCIN" имеет пустую БЗ. Такие системы предлагают дружественный интерфейс как эксперту, инженеру по знаниям, так и пользователю по наполнению БЗ и проведению консультации. Они позволяют выполнить отладку и тестирование БЗ. Другими словами, создать прототип ЭС. Коммерческая версия ЭС предполагает ее сертификацию и промышленную эксплуатацию.

Диапазон проблем, которые могут быть решены ЭС, обширен. Основные классы задач, решаемых ЭС: диагностика, прогнозирование, идентификация, управление, проектирование, мониторинг. Предметные области, в которых ЭС достигли широкого применения: медицина, компьютерная техника, военное дело, экономика, геология.

Примером оболочки для построения ЭС является система "КАРКАС" [2 – 6]. С помощью этой системы могут быть разработаны прототипы ЭС для любой предметной области, в которой для решения задачи необходимо сделать выбор среди определенного набора вариантов, а процесс достижения этого решения основан на логических шагах.

Инструменты системы "КАРКАС" используются для создания вероятностных, основанных на знаниях прототипов ЭС.

Современные ЭС широко используются для тиражирования опыта знаний экспертов практически во всех сферах экономики. Например, прецедентная экспертная система (ПЭС) как инструмент инновационного управления персоналом. Такая система может сама выделять наиболее характерные для группы работников качества, степень их выраженности и создавать нелинейные модели должностей.

Применение прецедентов позволило уменьшить число диагностируемых параметров. ПЭС имеют наряду с БЗ и базу прецедентов (результаты обследований в несколько сотен тысяч человек).

ЭС приходят к своим решениям во многом на основе человеческих наблюдений и фактически, наряду с математическими алгоритмами, используют человеческую логику для принятия решений. И в этом их огромное и принципиальное преимущество.

Ключевая роль ЭС в реинжиниринге бизнес-процессов состоит в том, что они позволяют пользователям заменить собой экспертов и узких специалистов, уменьшая тем самым количество людей, занятых в процессе, а следовательно, уменьшая число задержек и ошибок, возникающих в ходе взаимодействия между людьми.

Страховые компании преобразовали процесс выдачи страхового полиса, сделав так, что большая часть процесса проходит по телефону, и нет необходимости в специалистах, принимающих решения на основе оценки риска и особых обстоятельств.

Предпосылки широкого применения ЭС в экономике таковы:

количество профессиональных задач неуклонно растет. Сегодняшние выпускники экономических вузов преимущественно ориентированы на эксплуатацию компьютерных программ, а не на креативное решение экономических задач;

существуют различные формы работы, нацеленные на решение именно творческих задач: тренинги, консультации, экспертные системы, Internet-форумы;

появился ряд инструментальных средств по решению креативных задач ("ТРИЗ" [7], "КАРКАС"), использующих методические подходы к созданию БЗ и позволяющих эффективно решать ряд определенных задач в экономической предметной области;

в экономике образовался огромный рынок принятия решений.

Разработаны и модифицируются следующие учебные БЗ студентами старших курсов как индивидуальные научно-исследовательские проекты с применением инструментального средства "КАРКАС" по дисциплинам: "Управление знаниями", "Системы искусственного интеллекта" [5; 6]:

БЗ для выбора коммерческого банка;
БЗ для страхования коммерческих кредитов;
БЗ для выбора поставщиков продукции;
БЗ для выбора стратегии ценообразования;
БЗ для оценки кредитоспособности заемщика;
БЗ для оценки кредитоспособности предприятия;
БЗ для выбора депозита;
БЗ для оценки финансового состояния предприятия;
БЗ для выбора продукции;
БЗ для управления маркетингом;
БЗ для подбора кадров;
БЗ для подбора пакета туристических услуг.

Учебные БЗ служат наглядными методическими материалами для изучения работы системы "КАРКАС" [7; 8].

База знаний для выбора коммерческого банка.

Постановка задачи. Разработать БЗ по подбору банка для финансового обслуживания предприятия в зависимости от его потребностей в проведении кассово-расчетных, кредитных, депозитных, трастовых операций.

Назначение прототипа ЭС – это консультирование по подбору коммерческого банка для финансового обслуживания предприятия.

Сфера применения прототипа ЭС – это различные предприятия, которые нуждаются в финансовом обслуживании банками.

Цель прототипа ЭС – подбор наиболее оптимального варианта банка для финансового обслуживания предприятия в зависимости от его потребностей в проведении кассово-расчетных, кредитных, депозитных, трастовых операций.

Исходные данные:

для анализа деятельности предприятия – это характер производственной, сбытовой, закупочной деятельности, наличие или отсутствие свободных денежных средств;

для определения платежеспособности банка – это собственные средства, активы банка;

для определения ликвидности банка – это средства на расчетных, текущих и депозитных счетах и в кредиторской задолженности, а также суммы гарантий и поручительств, предоставленных банком.

Ожидаемые результаты (список возможных значений цели консультации):

требования к финансовому обслуживанию предприятия – это срочность денежных платежей, формы денежных платежей (наличные, безналичные), депозитные, кредитные, кассово-расчетные или трастовые операции;

требования к банкам – это платежеспособен или не платежеспособен, ликвиден или неликвиден.

Идентификация предметной области. Обязательными для каждого коммерческого банка являются следующие экономические нормативы, устанавливаемые Национальным банком Украины и определяющие надежность данного банка:

платежеспособность банка;
показатели ликвидности баланса;
максимальный размер риска на одного заемщика;
размер обязательных резервов, размещаемых в Национальном банке Украины.

При выборе коммерческого банка предприятие, как правило, опирается на следующие показатели:

надежность банка;
какая форма платежа подходит для предприятия: наличная или безналичная;
операции, которые желает осуществлять предприятие;
форма расчета, предпочитаемая предприятием.

База знаний для страхования коммерческих кредитов.

Постановка задачи. Страховая организация принимает на себя определенную долю возможного риска. Следовательно, любому предприятию в этих условиях необходима надежная защита от риска неплатежа со стороны партнера.

Назначение прототипа ЭС – это определение условий страхования кредита предприятия страховой компанией (предоставление льгот, страхование на обычных условиях, отказ) и расчет конкретных тарифов в зависимости от принятых условий.

Сфера применения прототипа ЭС – это оценка рисков коммерческого кредитования. Покрываемые риски: наступление банкротства контрагента страхователя; длительная просрочка платежа со стороны контрагента.

Пользователи: контрагент, страхователь.

Класс решаемых проблем: анализ условий страхования кредита предприятия.

Критерии эффективности и ограничения показателей: к результирующим экономическим показателям данной задачи относятся вычисляемые конкретные тарифы в зависимости от принятых условий страхования.

Цель страхования кредитов – это уменьшение или устранение для страхователей кредитных рисков.

Объектом страхования являются имущественные интересы страхователя, связанные с возможностью наступления убытков в результате неисполнения его контрагентом обязательств по контракту.

Ожидаемые результаты. Результатом оценки рисков коммерческого кредитования может быть предоставление льгот, страхование на обычных условиях либо отказ от страхования.

Подцели (промежуточные цели): оценка размера риска и вычисление тарифных коэффициентов на основе анализа исходных факторов.

Исходные данные (факторы): срочность, размер и условия предоставления кредита, возможность предоставления льгот, опыт предшествующего кредитования.

Особенности решения задач. Кредитный риск является функцией многих переменных: колебания цен, курса, общих экономических и политических условий, благонадежности предпринимателя.

Идентификация предметной области. Страхование коммерческих кредитов — это создание за счет денежных средств государства, предприятий, организаций, граждан специальных резервных фондов, предназначенных для возмещения ущерба, потерь, вызванных неблагоприятными событиями, несчастными случаями.

Для задания оценки возможных условий предоставления страхового кредита общепринятым методом является балльная оценка по ряду параметров:

размер страховых операций;
форма кредита;
срок, на который предоставляется кредит;
положение экспортера и производителя в коммерческой среде;
экономическое состояние страны импортера.

Для лица, принимающего решение, количественная оценка страховых компаний по вышеприведенным параметрам неудобна. Для альтернативного решения разработана БЗ для выбора страховой компании.

Концептуализация предметной области. Выбор страховой компании основывается на исследовании предлагаемых условий кредитования и разбивается на следующие этапы:

анализ опыта предшествующего кредитования;
анализ благонадежности предпринимателя;
анализ колебания уровня цен;
анализ вероятности погашения кредита в установленные сроки.

База знаний для оценки конкурентоспособности продукции.

Постановка задачи. Для оценки конкурентоспособности продукции маркетологи предприятия исследуют рынок, товары, конкурентов, потребителей, чтобы добиться оптимального соотношения цена/качество.

Назначение прототипа ЭС: консультирование.

Сфера применения: маркетинговая деятельность.

Класс решаемых проблем: анализ и прогнозирование.

Цель прототипа ЭС: найти самую конкурентноустойчивую продукцию.

Ожидаемые результаты: помощь в принятии правильного решения о том, какой товар производить и что делать с неконкурентоспособной продукцией руководителю фирмы или маркетологу.

Исходные данные: различные экономические, эргономические, технические, эксплуатационные характеристики товаров, данные о покупателях и заказчиках.

Особенности решения задач: существуют различные подходы к математическому моделированию конкурентоспособности продукции.

Идентификация предметной области. Подавляющее большинство компаний повышает конкурентоспособность продукции совершенствованием управления как организацией, так и ресурсами, добиваясь оптимального соотношения цена/качество.

База знаний для оценки кредитоспособности заемщика.

Постановка задачи. Методики, применяемые для оценки кредитоспособности, различны, но все они в той или иной степени позволят определить:

организационно-экономическую характеристику заемщика;

кредитную историю заемщика.

Не менее важным является анализ качественных показателей заемщика, таких, как: оценка состояния отрасли заемщика, оценка роли заемщика в регионе, оценка экономической, политической и технической политики организации.

Заметим, что для оценки заемщика общепринятым методом выступает балльная оценка по ряду параметров.

Назначение прототипа ЭС: консультирование по поводу выбора заемщиков – оценка кредитоспособности заемщика.

Цель: повышение качества результата выбора заемщиков, повышение качества и достоверности информации о данных, о заемщиках, повышение оперативности обработки этой информации.

Сфера применения: банки, кредитный отдел банка.

Класс разрешимых проблем: анализ выбора заемщика, выбор и отнесение заемщика к конкретному классу кредитоспособности.

Исходные данные (факторы): информация данных заемщиков: пакет документов, портфель кредитных заявок, кредитная история заемщика, рыночная позиция, данные об эффективности управления и деловых качествах руководства, обеспечение кредита – заставы, гарантии, поручительства.

Критерии эффективности: соответствие условий кредитования принятым требованиям.

Ожидаемые результаты: требования к условиям кредитования, эффективная оценка кредитоспособности заемщика.

База знаний для подбора кадров.

Постановка задачи. Система работы с кадрами должна быть спланирована таким образом, чтобы добиваться постоянного увеличения в составе кадров предприятия тех людей, кто обладает хорошими знаниями, квалификацией, физическими данными.

Назначение прототипа ЭС – это консультирование по поводу выбора кандидата на вакантную должность; работников кадровых служб, руководителей подразделений и фирм, консультантов по управлению, имиджмейкеров.

Цель: повышение качества результата выбора кандидатов, повышение качества и достоверности информации о кандидатах, повышение оперативности обработки этой информации.

Сфера применения: предприятия и фирмы.

Класс разрешимых проблем: подбор кадров на основании определенных критериев.

Ожидаемые результаты: эффективный подбор персонала по принятым требованиям.

Идентификация предметной области. Проблема по подбору персонала возникает в компаниях, не успевающих перестроить свою кадровую политику в соответствии с меняющимися рыночными условиями.

Требования к прототипу ЭС по подбору кадров. Для задания оценки кадров предприятия общепринятым методом является бальная оценка по ряду параметров: коммуникабельность, образование, интеллектуальный уровень, стаж работы, лидерские качества, уверенность в себе, состояние здоровья.

База знаний для подбора пакета туристических услуг.

Постановка задачи. Создать БЗ, которая позволит клиенту туристической фирмы по задаваемым вопросам определить наиболее оптимальный туристический пакет на основе анализа туристических предложений, которые имеются в наличии у туристической фирмы.

Требование к прототипу ЭС. Для задания выбора пакета туристических услуг общепринятым методом является оценка по ряду составляющих, которые влияют на критерии выбора клиентом пакета туристических услуг: ценовая составляющая, цель поездки, перевозка туристов, проживание туристов, питание туристов.

Назначение системы – это консультирование по поводу выбора пакета туристических услуг; выбор на основании определенных критериев наиболее выгодного для клиента пакета туристических услуг.

Цель прототипа ЭС – это повышение качества результата выбора пакетов туристических услуг, повышение качества и достоверности информации о наличии предложений на рынке туристических услуг, повышение оперативности обработки этой информации.

Сфера применения: туристические фирмы.

Класс разрешимых проблем: анализ существующих предложений на рынке туристических услуг, подбор пакета туристических услуг на основании определенных критериев.

Исходные данные:

информация об имеющихся пакетах туристических услуг: ценовые рамки пакета, наличие "горящих путевок", типы отдыха, виды транспорта, типы заведений проживания, питания;

данные о классах гостиниц, типах номеров, о классах мест в самолетах, типах поездов и классах вагонов в них, о классах заведений питания.

Критерии эффективности: соответствие условий, выдвигаемых клиентом, принятым требованиям.

Ожидаемые результаты: эффективный подбор пакета туристических услуг по заданным параметрам.

Идентификация предметной области. Формы и виды туризма разнообразные. Они зависят от ряда факторов: возраста, пола, состояния здоровья, уровня духовного развития, личных вкусов, материального состояния, разнообразности природных условий и сезонности.

Все прототипы ЭС относятся к классу "Decision Making Support Systems".

Литература: 1. Гаврилова Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский. – СПб.: Питер, 2000. – 384 с. 2. Бурдаєв В. П. Методичні рекомендації до використання експертно-навчальних систем для тестування знань з курсу "Інформатика та комп'ютерна техніка" для студентів усіх спеціальностей всіх форм навчання. — Харків: Вид. ХНЕУ, 2006. 3. Бурдаев В. П. Мультиагентная система в обучении // Тезисы VII Международной конференции ИМС'2006. – 2006. – С. 182 – 185. 4. Бурдаев В. П. Методика разработки баз знаний на основе системы "КАРКАС" // Научно-теоретический журнал "Искусственный интеллект". – 2007. – №3. – С. 70 – 80. 5. Бурдаев В. П. Управление знаниями в системе самостоятельной работы студентов на экономических специальностях // Управління розвитком. – 2007. – №7. – С. 166 – 168. 6. Бурдаєв В. П. Методичні рекомендації до проведення контроля знань на базі інструментального засобу "КАРКАС" з навчальних дисциплін "Інформатика і комп'ютерна техніка" та "Інформатика" для студентів напрямів підготовки 0501 "Економіка і підприємництво" та 0502 "Менеджмент" усіх форм навчання. – Харків: Вид. ХНЕУ, 2007. – 160 с. 7. Викентьев И. Л. Система "Триз-Шанс". Экспертные системы для принятия бизнес-решений // http://www. triz-ri. ru/themes/school/school27.asp – 17.11.2007 г. 8. Бурдаев В. П. Построение базы знаний для анализа финансового состояния предприятия в ЭОС "КАРКАС". Искусственный интеллект. Интеллектуальные и многопроцессорные системы – 2004 // Материалы Международной научной конференции. Т. 2. – Таганрог: Изд. ТРТУ, 2004. – С. 205 – 207.

Баранник В. В.

Хаханова А. В.

УДК 621.327:681.5

КОМБИНАТОРНАЯ МОДЕЛЬ ДВОИЧНЫХ МАТРИЦ

Существующие подходы относительно компактного представления двоичных данных не адекватны современным требованиям процессов функционирования информационных систем [1; 2]. Увеличиваются объемы данных, которые предназначены для хранения и передачи в информационно-регистрирующих системах. Основной причиной является организация сжатия двоичных данных на основе устранения вероятностных видов избыточности. В то же время количество такой избыточности зависит от типа законов распределения вероятностей появления символов в сообщении. Это приводит к снижению степени сжатия данных.

Поэтому **актуальной научной задачей** является сокращение объемов двоичных данных без внесения погрешности.

Цель статьи − обоснование выбора подхода для построения технологии компрессии двоичных данных.

Для дополнительного увеличения коэффициента сжатия, обрабатываемых двоичных данных предлагается дополнительно проводить сокращение избыточности в двоичных матрицах $\mathbf{G}$, $\mathbf{G}=\{\mathbf{g}_{\mathbf{k}\ell}\}$, $\mathbf{k}=\overline{\mathbf{1,n}}$, $\ell=\overline{\mathbf{1,n}}$, $\mathbf{g}_{\mathbf{k}\ell}\in\{\mathbf{0;1}\}$, где $\mathbf{g}_{\mathbf{k}\ell}$ – $(\mathbf{k};\ell)$-й элемент матрицы знаков. Двоичные матрицы имеют низкую избыточность $\mathbf{R}_{\text{ст}}$, определяемую на основе учета статистических закономерностей $\mathbf{R}_{\text{ст}}=(\mathbf{H}_0-\mathbf{H}_{\text{ст}})/\mathbf{H}_0\rightarrow\mathbf{0}$, где $\mathbf{H}_0$ − количество информации, в среднем приходящееся на один элемент матрицы, для случая, когда закономерности не выявлены, $\mathbf{H}_0=\mathbf{1}$ бит; $\mathbf{H}_{\text{ст}}$ − среднее

количество информации, содержащееся в одном элементе с учетом ограничений на закон распределения вероятностей $p_{k\ell}$ появления элементов $g_{k\ell}$: $H_{ст} = p(0)\ell og_2 p(0) + p(1)\ell og_2 p(1) \to H_0$, где $p(0)$, $p(1)$ – вероятности появления соответственно нулевого и единичного элементов. Это снижает потенциальные возможности относительно обеспечения необходимой степени компрессии двоичных матриц. Следовательно, сжатие двоичных матриц достигается за счет сокращения комбинаторной избыточности, независящей от статистических свойств матриц G.

Анализируемая характеристика двоичных матриц должна учитывать взаимное расположение нулевых и единичных элементов и их количество. Причем количество нулевых элементов может равняться количеству единичных. Количество информации H в двоичных последовательностях с учетом анализируемых ограничений должно удовлетворять следующим требованиям:

1) количество информации на один элемент должно быть меньшим единицы для источника информации с равномерным появлением единиц и нулей:

$$H <<< 1 \text{ для } p(0) \approx p(1); \tag{1}$$

2) величина H для произвольных значений анализируемой характеристики η должна быть меньше единицы:

$$\max_{\eta_{min} \le \eta \le \eta_{max}} \{H\} < 1, \tag{2}$$

где η_{min}, η_{max} – соответственно минимальное и максимальное значения величины η.

Предлагается рассматривать выявления закономерностей на основе характеристики количества серий η. Признак серии задается системой выражений:

$$\begin{cases} g_{k-1,\ell} \ne g_{k\ell} \to k \le n; \\ g_{k,\ell} \ne g_{1,\ell+1} \to k > n. \end{cases}$$

Вычисление количества серий единиц η для ν элементов матрицы G:

на нулевом шаге $g_{0,\ell} = 0$; $\eta_\ell = 0$;

на k-м шаге значения числа серий увеличиваются на 1, $\eta_{k\ell} = \eta_{k-1,\ell} + 1$, если $g_{k-1,\ell} < g_{k\ell}$;

в противном случае $\eta_{k\ell} = \eta_{k-1,\ell} + 0$, если $g_{k-1,\ell} \ge g_{k\ell}$;

для конечного шага при $k = \nu$ получаем искомое значение количества серий единиц $\eta = \eta_\nu$ для j-го столбца.

Количество $V_{\nu,\eta}$ двоичных последовательностей G_ν, содержащих ν элементов и η серийных перепадов, равно [3; 4]:

$$V_{\nu,\eta} = (\nu+1)!/(2\eta)!\,(\nu+1-2\eta)!. \tag{3}$$

В соответствии с выражением (3) количество информации H, в среднем приходящееся на один элемент двоичной последовательности с η сериями единиц, равно:

$$H = \Big(\sum_{\xi=1}^{\nu+1} \ell og_2 \xi - \sum_{\xi=1}^{2\eta} \ell og_2 \xi - \sum_{\xi=1}^{\nu+1-2\eta} \ell og_2 \xi\Big)/\nu. \tag{4}$$

Рассмотрим соответствие величины H условиям (1) и (2):

1) для фиксированного ν максимальное значение $V_{\nu,\eta}$ двоичных последовательностей достигается для $\eta = \eta_{ср} = [(\nu+1)/4]$. Это вытекает из того, что величина $V_{\nu,\eta}$ для $0 \le \eta \le [(\nu+1)/2]$ имеет один максимум в области среднего значения η. Поэтому для проверки условия (2) необходимо определить значение величины $V_{\nu,\eta_{ср}}$:

$$V_{\nu,\eta_{ср}} = \begin{cases} (\nu+1)!/(\nu/2)!\,(\nu/2+1)!, & \to \nu \bmod(2) = 0; \\ (\nu+1)!/((\nu+1)/2)!\,((\nu+1)/2)!, & \to \nu \bmod(2) \ge 1, \end{cases} \tag{5}$$

где $\nu \bmod(2) = 0$, $\nu \bmod(2) \ge 1$ – условия, когда величина ν принимает соответственно четные и нечетные значения.

Значит для $\eta = \eta_{ср} = [(\nu+1)/4]$ величина H будет принимать максимальное значение, равное:

если $\nu \bmod(2) = 0$, то

$$H_{\nu,\eta_{ср}} = \Big(\sum_{\xi=1}^{\nu+1} \ell og_2 \xi - 2\sum_{\xi=1}^{\nu/2} \ell og_2 \xi - \ell og_2 (\nu/2+1)\Big)/\nu;$$

если $\nu \bmod(2) \ge 1$, то

$$H_{\nu,\eta_{cp}} = (\sum_{\xi=1}^{\nu+1} \ell og_2 \xi - 2 \sum_{\xi=1}^{(\nu+1)/2} \ell og_2 \xi)/\nu, \quad (6)$$

где $H_{\nu,\eta_{cp}}$ – количество информации, приходящееся на один элемент матрицы в случае, когда число серий единиц равно $\eta = \eta_{cp} = [(\nu+1)/4]$.

Условие (2) выполняется, если

$$H_{\nu,\eta_{cp}} < 1. \quad (7)$$

Правая часть неравенства (7) соответствует варианту, когда количество допустимых двоичных последовательностей равно 2^{ν}. Поэтому неравенство (7) будет выполняться для

$$V_{\nu,\eta_{cp}} < 2^{\nu}. \quad (8)$$

Рассмотрим сумму величин $V_{\nu,\eta}$ по всему диапазону значений числа серий единиц $0 \le \eta \le [(\nu+1)/2]$:

1. Если ν четное, то $\eta = \overline{0, \nu/2}$. Введем вспомогательные переменные $\alpha = (\nu+1)$ и $\beta = 2\eta$, тогда

$$\sum_{\beta=0}^{(\alpha-1)} (\alpha)!/((\beta)!\,(\alpha-\beta)!). \quad (9)$$

Переменная β принимает все значения в диапазоне $\beta = \overline{0, (\alpha-1)}$. В то время как величина 2η принимает в этом диапазоне только положительные четные значения. Поэтому

$$\sum_{\eta=0}^{\nu/2} V_{\nu,\eta} = \sum_{\beta=0}^{(\alpha-1)} h_{\alpha,\beta}, \quad (10)$$

$$h_{\alpha,\beta} = \begin{cases} (\alpha)!/((\beta)!\,(\alpha-\beta)!), \to (-1)^{\beta} = 1; \\ 0, \qquad\qquad\qquad \to (-1)^{\beta} = -1. \end{cases}$$

Тогда с учетом свойства сочетаний без повторений

$$\sum_{\beta=0}^{\alpha} ((-1)^{\beta}(\alpha)!)/((\beta)!\,(\alpha-\beta)!) = 0 \quad (11)$$

получим $\sum_{\eta=0}^{\nu/2} V_{\nu,\eta} = 2^{\alpha-1} = 2^{\nu}$. В то же время $V_{\nu,\eta_{cp}} < \sum_{\eta=0}^{\nu/2} V_{\nu,\eta}$. Отсюда следует, что для четного ν неравенство (8) выполняется.

2. Если ν нечетное, то $\eta = \overline{0, (\nu+1)/2}$, а

$$\sum_{\eta=0}^{(\nu+1)/2} V_{\nu,\eta} = \sum_{\eta=0}^{(\nu+1)/2} \frac{(\nu+1)!}{(2\eta)!\,(\nu+1-2\eta)!}.$$

С учетом свойств, заданных соотношениями (10) и (11), получим

$$\sum_{\eta=0}^{\nu/2} V_{\nu,\eta} = 2^{\alpha-1} = 2^{\nu}.$$

Следовательно, неравенство (8) выполняется для нечетного ν.

Таким образом, условие (2) для предлагаемой количественной характеристики "число серий единиц" выполняется.

Рассмотрим условие (1) применительно к характеристики "число серий единиц". Количество $V(s)_{\nu,\eta}$ двоичных последовательностей для числа единиц, равного s, распределенных по η сериям, равно

$$V(s)_{\nu,\eta} = \frac{(s-1)!}{(\eta-1)!\,(s-\eta)!} \times \frac{(\nu-s+1)!}{(\eta)!\,(\nu-s+1-\eta)!}, \quad \eta = \overline{0, \min(s; \nu/2)}. \quad (12)$$

В случае равных вероятностей $p(0) \approx p(1)$ имеем одинаковое количество нулевых и единичных элементов, равное $\nu/2$. Для такого условия выражение (12) будет иметь вид:

1. Если ν — четное:

$$V(\nu/2)_{\nu,\eta} = \frac{((\nu/2)-1)!}{(\eta-1)!((\nu/2)-\eta)!} \times \frac{((\nu/2)+1)!}{(\eta)!((\nu/2)+1-\eta)!}, \quad \eta = \overline{0, s}. \quad (13)$$

Поскольку сомножители в правой части выражения (13) представляют собой сочетания без повторений, то они достигают максимума при $\eta/2$. Значит максимальное значение величина $V(s)_{\nu,\eta}$ при фиксированных ν и s достигает для $\eta = s/2 = \nu/4$:

$$V(\nu/2)_{\nu,\nu/4} = \frac{((\nu/2)-1)!}{((\nu/4)-1)!\ ((\nu/4))!} \times \frac{((\nu/2)+1)!}{((\nu/4))!((\nu/4)+1)!}. \quad (14)$$

В соответствии с данным выражением количество информации $\overline{H}(\nu/2)_{\nu,\nu/4}$, приходящееся на один элемент двоичной последовательности, содержащей $\eta = \nu/4$ серий единиц и $\nu/2$ единичных элементов, находится по формуле:

$$\overline{H}(\nu/2)_{\nu,\nu/4} = \log_2\left(\frac{((\nu/2)-1)!}{((\nu/4)-1)!((\nu/4))!} \times \frac{((\nu/2)+1)!}{((\nu/4))!((\nu/4)+1)!}\right)/\nu. \quad (15)$$

Поскольку количество η серий единиц дополнительно ограничено величиной s, то выполняется неравенство:

$$\sum_{\eta=1}^{s} V(s)_{\nu,\eta} = \sum_{\eta=1}^{\nu/2} V(\nu/2)_{\nu,\eta} < \sum_{\eta=0}^{\nu/2} V_{\nu,\eta}. \quad (16)$$

Правая часть неравенства (16) имеет ограничение $\sum_{\eta=0}^{\nu/2} V_{\nu,\eta} = 2^{\nu}$. Значит $\sum_{\eta=1}^{s} V(s)_{\nu,\eta} < 2^{\nu}$.

Откуда получаем:

$$2\sum_{\xi=1}^{((\nu/2)-1)} \log_2 \xi - \sum_{\xi=(\nu/2)}^{((\nu/2)+1)} \log_2 \xi - 2\sum_{\xi=1}^{((\nu/4)-1)} \log_2 \xi - \sum_{\xi=(\nu/4)}^{((\nu/4)+1)} \log_2 \xi - 2\sum_{\xi=1}^{(\nu/4)} \log_2 \xi < \nu.$$

Следовательно, максимальное значение количества информации $\overline{H}(\nu/2)_{\nu,\nu/4}$ будет меньшим единицы. Условие (1) выполняется. По аналогии доказывается, что условие (1) выполняется для нечетного ν.

Таким образом, двоичные матрицы данных имеют комбинаторную избыточность, обусловленную ограничениями на число серий единиц.

Построена комбинаторная модель оценки информативности двоичных матриц данных. Обосновано, что учет закономерностей по числу серий единиц позволяет сократить избыточность в условиях нестационарности статистических свойств исходных фрагментов данных.

Литература: 1. Прэтт У. Цифровая обработка изображений: Т. 1, 2. – М.: Мир, 1985. – 736 с. 2. Ватолин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / В. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с. 3. Королев А. В. Оценка количества информации изображения по числу серий одинаковых элементов / А. В. Королев, В. В. Баранник // Системи обробки інформації. – Харків: НАНУ, ПАНМ, ХВУ. – 2002. – Вип. 2(18). – С. 43 – 46. 4. Баранник В. В. Рекуррентное двухпризнаковое двоичное полиадическое кодирование / В. В. Баранник, В. В. Юдин // Открытые информационные и компьютерные интегрированные технологии. – Харьков: НАУ "ХАИ". – 2006. – Вып. 33. – С. 22 – 28.

УДК 004.056.5

Хома В. В.

Гарасим Ю. Р.

ПОБУДОВА ЗАХИЩЕНОЇ ВІДОМЧОЇ ТЕЛЕФОННОЇ МЕРЕЖІ НА ОСНОВІ МІНІ-АТС CORAL І ФІРМИ TADIRAN

За останні роки у сфері телекомунікацій і телефонного зв'язку відбулися справді грандіозні зміни, зумовлені широким упровадженням цифрових технологій. При цьому, крім беззаперечних переваг цифрового зв'язку (висока якість та ширший спектр послуг), додалися і нові проблеми, зокрема, пов'язані із захистом інформації від витоку технічними каналами.

За тривалий час використання телефонних мереж, побудованих на аналоговому обладнанні, було створено широкий спектр пристроїв, призначених для захисту телефонного зв'язку від несанкціонованого доступу і побічних електромагнітних випромінювань та наводок. Проте це обладнання не може бути ефективно використане для захисту нових цифрових пристроїв, що пов'язано, насамперед, із зміною вигляду та спектру сигналів і алгоритмами їх перетворення. До акустичних перет-

---

ворювачів, що присутні в аналогових системах, додалися нові структурні елементи, такі, як аналого-цифрові й цифро-аналогові перетворювачі, пристрої цифрового оброблення. Одним із головних каналів витоку став канал обміну оброблюваної інформації між центральним процесором телефонного апарату та цифровою станцією. Спеціально проведені дослідження показали, що зони випромінювання робочих сигналів, які містять оброблювану інформацію, можуть бути перехоплені на відстані до 30 метрів. Крім того, небезпечні сигнали (з точки зору інформаційної безпеки) з'являються в мережах електроживлення [1].

Аналіз телефонного зв'язку з позицій інформаційної безпеки

Телефонний тракт утворюється шляхом фізичного з'єднання абонентської лінії, елементів комутаційного поля АТС, каналів з'єднувальних ліній та систем передачі. Перехоплення голосових повідомлень у з'єднувальних лініях і магістральних каналах систем передачі є складним через потребу демультиплексування групових сигналів. АТС – це також досить захищений елемент телефонного тракту, особливо порівняно із абонентською телефонною лінією (АТЛ). Проте загрози для інформації на АТЛ є неоднаковими на різних її ділянках.

Найвразливішою з погляду перехоплення та блокування інформації виступає ділянка абонентської телефонної лінії від телефонної розетки до розподільчої коробки, виконана двопровідним телефонним проводом.

У телефонних мережах загального користування кожна АТЛ асоціюється із конкретним абонентом цієї мережі, тобто аутентифікація абонентів здійснюється лише на основі фізичного підключення до АТЛ. Зважаючи на відкритість та доступність прикінцевих ділянок АТЛ, існує досить велика загроза інформаційній безпеці шляхом несанкціонованих підключень.

Цифрові комунікаційні системи Coral™ FlexiCom™

Складовою частиною Coral™ FlexiCom™ є система технічного захисту інформації. Вона призначена для технічного забезпечення нормативно встановленого рівня захищеності системних та інформаційних ресурсів і дозволяє здійснювати неперервний контроль за ефективністю функціонування засобів захисту, підтримувати необхідний рівень захищеності інформаційних ресурсів на всіх технологічних етапах обробки викликів, а також в усіх режимах функціонування та надання послуг (при проведенні ремонтних і регламентних робіт).

Технічна політика безпеки дозволяє системі технічного захисту інформації відповідати специфічним нормативним вимогам за захищеністю інформаційних ресурсів у телекомунікаційних системах. В Україні штатна система технічного захисту інформації Coral™ FlexiCom™ сертифікована відповідними державними органами на її відповідність вимогам чинної системи технічного захисту інформації з рівнем довіри Е3 для обробки конфіденційної інформації [2]. Це означає, що для коректності захисту відомчої телефонної мережі необхідним є дотримання вимог до довірчих оцінок, що встановлені НД ТЗІ 2.5-003-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок корекції реалізації захисту".

Специфікації довірчих оцінок необхідні для визначення рівнів довіри до коректності розробок та реалізацій систем ТЗІ в оцінюваних АТС, якщо оцінка рівнів довіри виконується згідно з базовою методикою оцінки захищеності інформації на АТС НД ТЗІ 3.7-002-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)", що ґрунтується на єдиних (уніфікованих) для Європейського Союзу "Критеріях оцінки безпеки систем інформаційної техніки – ITSEC" [3].

Оскільки програмно-керовані АТС належать до класу захищених систем інформаційної техніки, то методика оцінки їх захищеності в повній мірі визначається вищезгаданими критеріями ITSEC з урахуванням специфічних особливостей АТС як інформаційно вразливого об'єкта. Для одержання впевненості в тому, що АТС забезпечує очікувану якість захисту інформаційних ресурсів, необхідне підтвердження досягнутого рівня якості такого захисту з боку незалежного експерта [4].

Мережі зв'язку на основі Coral™ FlexiCom™ обслуговують адміністративні комплекси міністерства оборони США Pentagon, підрозділи МВС України, Білорусії, Росії, органи Державної податкової служби і поліції Росії, агентства державного зв'язку при Комітеті національної безпеки Казахстану [5].

Визначення моделі загроз

Загрозами для інформації, що циркулює на АТС, є:

порушення конфіденційності, цілісності, доступності або відмова в обслуговуванні;

порушення спостережності або керованості;

несанкціоноване користування інформаційними ресурсами.

Щодо телефонного зв'язку, то загроза конфіденційності проявляється у підслуховуванні телефонних розмов (режим піднятої телефонної трубки), а також у прослуховуванні приміщень, де знаходиться телефонний апарат (режим відкладеної телефонної трубки).

Загрози для інформації на АТС здійснюються через такі канали спеціальних впливів [6]: кількісну недостатність компонентів АТС; якісну недостатність компонентів АТС; навмисну або ненавмисну діяльності осіб, які, у свою чергу, впливають на елементи АТС з використання програмних і (або) технічних засобів; несправності апаратних елементів АТС; вихід за межі припустимих значень параметрів зовнішнього середовища функціонування АТС (у тому числі пов'язаних зі стихійними лихами, катастрофами та іншими надзвичайними подіями); помилки і некоректність дій суб'єктів доступу до ресурсів АТС на стадії її промислової експлуатації.

При виконанні технічного захисту інформації необхідним є дотримання принципів легітимності, комплексності, безперервності та мінімальної достатності захисту.

До основних функцій, що забезпечують захист інформацій в системі Coral I належать: введення особистого паролю для доступу до з'єднувальних ліній; блокування абонентів; наведення довідки під час розмови з зовнішнім абонентом; категоріювання абонентів; запис даних про з'єднання

(SMDR); контроль доступу до зовнішніх ліній; контроль доступу до груп зовнішніх ліній; контроль параметрів і функцій абонентів і ліній (зовнішніх та внутрішніх); розподіл зовнішніх ліній на групи та доступ до них; системна діагностика; секретний пароль для використання терміналу; встановлення обмеження виходу на міські/міжнародні лінії; встановлення обмежень для різних абонентів [7].

Технологічні аспекти технічного захисту інформації в системі Coral I:

1. Відкрита модульна структура побудови всіх пристроїв і програмного забезпечення, які утворюють єдиний універсальний програмно-апаратний комплекс.

2. Забезпечення техніко-експлуатаційної надійності системи як одного із основних показників за рахунок використання дублювання функцій управління, системи самодіагностики, що працюють у неперервному режимі, безперебійні джерела живлення й автоматичне переключення в аварійний режим, відсутність конструкції електромеханічних вузлів і агрегатів (систем вимушеної вентиляції чи кондиціонування, накопичувачів на жорстких дисках).

3. Децентралізований принцип обробки даних, при якому кожна периферійна плата і цифровий термінал мають власні процесори, а кількість периферійних процесорів прямо пропорційна розмірам самої станції. При цьому незалежно від розмірів станції робоче навантаження на будь-який із процесорів залишається сталим і контрольованим. Таким чином, якщо ємність периферійної схемотехніки залежить від ємності системи, то схеми загального керування практично однакові для всіх систем.

4. Універсальність роз'ємних місць для периферійних плат не залежить від ємності системи і додаткових кабінетів у системі Coral™ FlexiCom™.

5. Відсутність спеціальних вимог до службових приміщень (кондиціювання, температурні чи антистатичні показники, електрична або електромагнітна сумісність з іншими пристроями вузла зв'язку, обмеження щодо тривалості знаходження в цих приміщеннях технічного персоналу тощо) та забезпечення працездатності в діапазоні температур від −15□до +50□С і вологості до 95%.

Інформаційні аспекти технічного захисту інформації Coral I:

1. Багаторівневий принцип реалізації програмного забезпечення (ПЗ), що включає в себе системне ПЗ, ПЗ периферійного обладнання, ПЗ термінального обладнання і ПЗ опційних утиліт.

2. Уніфікованість системного програмного забезпечення для всіх базових систем різної ємності, яке знаходиться на Flash ПЗП і захищене відповідними ключами високої стійкості.

3. Використання високоефективного методу перевірки легітимності застосування системного програмного забезпечення, що реалізоване у вигляді шифратора − модуля авторизації програмного забезпечення SAU (Software Authorization Unit).

4. Високий рівень реалізації програмного забезпечення, яке, реалізовуючи всі системні, комутаційні та сервісні функції, займає мінімальні обсяги пам'яті й забезпечує максимально ефективний і простий програмний інтерфейс користувача.

5. Ефективні методи забезпечення схоронності всіх баз даних системи, в тому числі за рахунок їх автоматичного резервування за алгоритмом, що встановлюється адміністратором системи.

Література: 1. Коровин И. Защита информации в сетях цифровых АТС. – М., 1999. 2. www. flexi. com. ua. 3. НД ТЗІ 2.5-003-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок корекції реалізації захисту" // www.dstzi.ua. 4. НД ТЗІ 3.7-002-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)" // www.dstzi.ua. 5. CoralTM FlexiComTM. Гибкий путь к общению. – К., 2001. 6. НД ТЗІ 1.1-001-99 "Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення" // www.dstzi.ua. 7. Continuous Communication Systems. Coral Цифровая универсальная система связи. Общее описание. ECI Telecom BUSINESS SYSTEMS. – К., 2001.

УДК 004.491

Голубев В. А.

КИБЕРПРЕСТУПНОСТЬ − УГРОЗЫ И ПРОГНОЗЫ

Подобно многим революционным технологиям глобальная сеть Internet предоставляет огромные возможности как для прогресса, так и для злоупотреблений. Атаки в сети, мошенничества с пластиковыми платежными карточками, кражи средств из банковских счетов, корпоративный шпионаж, распространение детской порнографии − это лишь некоторые из преступлений, которые происходят в сети Internet. Такие противоправные деяния составляют для нашего государства, как и для многих других стран мира, значительную общественную опасность, реально угрожая информационной безопасности − составляющей национальной безопасности.

Национальная инфраструктура государства уже сегодня тесно связана с использованием современных компьютерных технологий. Ежедневная деятельность банковских и энергетических

систем, управления воздушным движением, транспортная сеть, даже скорая медицинская помощь находятся в полной зависимости от надежной и безопасной работы автоматизированных электронно-вычислительных систем.

Преступность в сфере использования компьютерных технологий ("киберпреступность") – это явление международного значения, уровень которого непосредственно зависит от уровня развития и внедрения современных компьютерных технологий, сетей их общего пользования и доступа к ним. Таким образом, стремительное развитие информатизации в Украине несет в себе потенциальную возможность использования компьютерных технологий из корыстных и других мотивов, что в известной мере ставит под угрозу национальную безопасность государства.

Основной целью киберпреступника является компьютерная система, которая управляет разнообразными процессами, и информация, что циркулирует в них. В отличие от обычного преступника, что действует в реальном мире, киберпреступник не использует традиционное оружие – нож и пистолет. Его арсенал – информационное оружие, все инструменты, которые используются для проникновения в сети, взлома и модификации программного обеспечения, несанкционированного получения информации или блокировки работы компьютерных систем. К оружию киберпреступника можно прибавить: компьютерные вирусы, программные закладки, разнообразные виды атак, которые делают возможным несанкционированный доступ к компьютерной системе. В арсенале современных компьютерных преступников есть не только традиционные средства, но и самое современное информационное оружие и оборудование; эта проблема уже давно пересекла границы государств и получила международное значение.

Вместе с последующим внедрением современных информационных технологий в Украине постоянно растет угроза как для государственных компьютерных систем, так и для частных организаций и отдельных граждан.

Особенную актуальность проблема киберпреступности приобрела в наше время. Социологические опросы в разных странах, и в первую очередь в высокоразвитых, показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые тревожат людей. Более того, по мнению специалистов, сегодня это явление составляет значительно более серьезную опасность, чем 5 лет назад, в связи с использованием преступниками новейших информационных технологий, а также через растущую уязвимость современного индустриального общества. Невзирая на усилия государств, которые направлены на борьбу с киберпреступниками, их количество в мире не уменьшается, а, напротив, постоянно растет.

Ни одно государство сегодня не способно противостоять этому злу самостоятельно. Неотложной выступает потребность активизации международного сотрудничества, для которого является актуальным, в частности, налаживание международно-правового механизма регуляции. Но, ввиду того, что в современных условиях значительная часть средств борьбы с киберпреступлениями, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт.

Отсутствие эффективных механизмов борьбы с киберпреступлениями определяется сегодня как одна из угроз национальной безопасности нашего государства. При таких обстоятельствах Украина, как независимое демократическое государство, не может стоять в стороне от проблем противодействия компьютерной преступности и, в частности, ее транснациональных (трансграничных) форм.

Рассмотрим типичные категории компьютерных преступлений и те негативные последствия, с которыми общество сталкивается уже сегодня.

Инсайдеры (Insiders) – лица, которые имеют доступ к внутренней информации. Чаще всего именно они негативно настроены против своих работодателей. Инсайдер (работающий или освобожденный сотрудник компании) является потенциальным преступником. Знакомый с тонкостями компьютерной системы компании, он имеет неограниченный доступ к системе с целью незаконного вмешательства в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей или с целью незаконного завладения информацией, которая является собственностью компании [1].

Как пример можно привести случай, когда Национальная библиотека медицинской литературы (National Library of Medicine – NLM), к которой обращаются сотни тысяч практикующих врачей и специалистов в отрасли медицины из всего мира для получения информации о заболевании, лечении, медикаментах, испытала нападение со стороны инсайдера. Тот осуществил несанкционированный доступ к главной системе защиты информации, загрузив сотни файлов, в том числе наиболее важные – категории "скорая помощь", и файлы программного обеспечения, от которых зависела бесперебойная работа системы. Эти нарушения привели к значительным негативным последствиям в работе всей системы и убыткам в размере 25 тыс. долларов. Расследование, проведенное ФБР США, установило лицо преступника, которым оказался Монтгомери Джон Грей (Montgomery Johns Gray) – программист, чей доступ в компьютерную систему был аннулирован компанией после его освобождения. Он совершил взлом через "черный вход", созданный им же в программном коде. Преступник был арестован ФБР как носитель угрозы обществу.

Хакеры (Hackers) также составляют большую опасность. Иногда они взламывают сети просто ради острых ощущений или ради завоевания авторитета в хакерских кругах. Но нередко это происходит с целью финансовой наживы и других злодеяний. Как правило, хакеры – прекрасные знатоки информационной техники, которые имеют неординарные способности, поэтому для них не

является проблемой манипулирования компьютерными системами на расстоянии: они не санкционировано перекачивают тексты и протоколы с World Wide Web на сайты компьютера жертвы. Преступления, когда происходит блокировка обслуживания (DDOS-атака), – еще одно доказательство того, что экономический саботаж полностью возможен при использовании надлежащих и доступных программных инструментов в сети Internet [1].

В последнее время участились политически мотивированные атаки на вебсайты и серверы электронной почты, которые за приемами выполнения дублируют "хакерство". В таких случаях группа или отдельные субъекты перегружают серверы электронной почты или стирают вебсайты для передачи политических сообщений. Хотя такие виды нарушений не приводят к повреждению операционных систем или сети, однако они становятся причиной сбоев работы электронной почты, что, в свою очередь, приводит к большим денежным расходам и блокировке доступа абонентов к вебсайтам, на которых находится ценная информация. Да, в 1996 году был совершен несанкционированный доступ к компьютерной системе вебсайта министерства юстиции США. Злоумышленники уничтожили содержание свыше 200 каталогов и разместили страницы с изображением Адольфа Гитлера, свастики, сцен порнографического характера и т. п.

В Украине ежегодно раскрывается около 500 преступлений в сфере использования компьютерных технологий.

В 2007 году наиболее распространенными преступлениями были: мошенничество с использованием компьютерной техники, несанкционированный сбыт и распространение информации с ограниченным доступом, несанкционированное вмешательство в работу компьютерных и телекоммуникационных систем, подделки банковских платежных карточек, а также мошенничество со стороны операторов связи и абонентов телекоммуникационных компаний.

Служба безопасности Украины только за первый месяц 2007 года возбудила 15 уголовных дел за преступления в сфере компьютерных технологий. В частности, представителями СБУ были задержаны продавцы информации с ограниченным доступом, базами телефонной сети 09, ГАИ МВД Украины, налоговой администрации, таможни.

В России в прошлом году было зафиксировано около 14 тысяч компьютерных преступлений. Чрезвычайно разнообразны компьютерные мошенничества – это ложные предложения товаров и услуг через Интернет, услуги по организации хакерских атак, аферы с электронными платежными картами и счетами клиентов электронных платежных систем. В прошлом году было совершено свыше 450 таких преступлений. Статистика показывает, что почти в 43% случаев жертвами компьютерных мошенников становятся участники онлайновых аукционов – когда покупатель клюет на недобросовестное предложение приобрести какой-нибудь товар по очень низкой цене, но с предоплатой.

Особую обеспокоенность вызывает безопасность Интернет. Необходимость привлечения внимания к проблеме безопасности в сети вызвана тем, что виртуальная среда давно сравнялась по опасности с реальной. Неприятности, приходящие из компьютера, примерно те же, что и в обычной жизни: вирусы, кражи и грабежи, хамство и преследование, вымогательства и угрозы, неэтичная и навязчивая реклама, терроризм и экстремизм. Украденные хакерами деньги уже давно считаются миллиардами, а к некоторым вирусам по нескольку месяцев не могут подобрать противоядия. "Отморозки" всех рангов и завихрений назначают свои встречи через сеть, там же отдают приказы об "акциях" и отчитываются об их исполнении (от очередного побитого "инородца" до взорванного дома) [2]. Таким образом, Всемирная сеть – идеальный источник информации и развлечений, который может стать для любого из нас и идеальным источником проблем.

Статистика говорит сама за себя:

86% атакуемых хакерами компьютеров – домашние; спам составляет 54% контролируемого трафика электронной почты в мире, в России – 82% трафика;

рост фишинговых (связанных с сетевым мошенничеством) сообщений на июнь 2006 года составил 81%;

18% обезвреженных образцов вредоносных вирусов – новые;

4,2 млн. сайтов – порнографические;

55% блоггеров пишут свои Интернет-дневники под псевдонимом, опасаясь негативных последствий в реальной жизни.

Пожалуй, наиболее уязвимыми для потока информационного мусора из Всемирной сети являются дети. Исследования показали, что 90% детей сталкивались в Интернете с порнографией, а 65% искали ее целенаправленно. Интерес к "клубничке" привел к тому, что 44% несовершеннолетних пользователей Интернета хотя бы раз подвергались сексуальным домогательствам в сети. Эти данные не покажутся столь удивительными, если иметь в виду, что половина детей выходят в Интернет без всякого контроля со стороны родителей или педагогов. Более того, как показывают опросы, большинство из них настолько доверчивы, что готовы предоставить "виртуальному другу" в Интернете свои личные данные (вплоть до пин-кодов кредиток родителей).

После того, как были созданы 217 тыс. программ, нацеленных на нанесение ущерба персональным компьютерам, мир организованной преступности осознал потенциальную выгоду от операций в киберпространстве и теперь сосредоточил усилия на похищении личных данных пользователей, отмечается в докладе "Десять основных угроз безопасности в 2007 году", подготовленном экспертами "МакАфи".

Проблема противодействия компьютерной преступности – это комплексная проблема. Сегодня законы должны соответствовать требованиям, предъявляемым современным уровнем развития технологий. С этой целью необходимо проводить целенаправленную работу по гармонизации

и совершенствованию законодательства, регулирующего распространение информации в телекоммуникационных сетях [3 – 5]. Одним из приоритетных направлений является также организация взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой.

Литература: 1. Голубев В. А. Одинадцатый Конгресс ООН: противодействие компьютерной преступности / Центр исследования компьютерной преступности // http://www. crime-research. ru/analytics/ crime_bangkok/. 2. Голубев В. А. Проблемы противодействия киберпреступности и кибертерроризму в Украине // Сб. научн. работ "Компьютерная преступность и кибертерроризм". – 2005. – Вып. 3. – С. 21 – 34. 3. Голубев В. А. Украина: вопросы противодействия компьютерной преступности // Сб. научн. работ "Компьютерная преступность и кибертерроризм". – 2004. – Вып. 3. – С. 8 – 18. 4. Голубев В. А. Компьютерная преступность — проблемы и решения / Центр исследования компьютерной преступности // http://www. crime-research. ru/articles /golubev_sept/. 5. Голубев В. А. Компьютерная преступность в странах СНГ (аналитический обзор) / Центр исследования компьютерной преступности // http://www. crime-research. ru/analytics/ rcrime_statistics/.

Калашников А. А.

УДК 351.86 (477)

НОВЫЙ ПОДХОД К ОПОВЕЩЕНИЮ НАСЕЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

В Законе Украины, описывающем правовые основы гражданской защиты (ГЗ), [1] указаны её основные задачи. Одной из них является организация защиты населения и территорий от чрезвычайных ситуаций (ЧС); предоставление неотложной психологической, медицинской и другой помощи пострадавшим; оперативное оповещение населения о возникновении или угрозе возникновения ЧС, своевременное достоверное информирование об обстановке, которая складывается, и мероприятиях, которые применяются для предотвращения ЧС и преодоления их последствий.

Все граждане обязаны принимать активное участие в выполнении мероприятий, которые будут вестись в этот период органами ГЗ, а именно: обеспечение своевременного получения сигналов, команд, распоряжений органов власти и ГЗ; осуществление противопожарных мероприятий; подготовка дома (квартиры) к защите от проникновения радиоактивной пыли и паров сильнодействующих ядовитых веществ; организация эвакуационных мероприятий; защита продуктов питания и воды от заражения; осуществление противоэпидемических мероприятий. Кроме того, в целях сокращения сроков доведения информации об угрозе радиоактивного и химического заражения, катастрофического затопления населения, которое находится на потенциально опасных объектах и непосредственно близ них, а также в транспортных средствах, решением начальников ГЗ оповещение указанного населения может быть возложено на начальников ГЗ соответствующих объектов и транспортных средств. При этом предусматривается возможность оповещения указанного населения также и территориальными органами.

Основное средство оповещения населения – передача сообщения по радио и телевиденью. На каждый случай ЧС местные органы ГЗ готовят приблизительные варианты сообщений, которые потом с учетом конкретных событий корректируются. Информация передается на протяжении 5 минут после подачи звуковых сигналов (сирена, гудки и др.). Выслушав сообщение управления (отдела) МЧС населения области (района, города), каждый должен действовать без паники и суеты в соответствии с полученными указаниями. Но данная ситуация рассмотрена при идеальном стечении обстоятельств: когда человек слышит данный сигнал, когда знает о сигнале оповещения и как на него реагировать, какие действия предпринять для самозащиты и помощи окружающим. Возникает вопрос о том, все ли слышат о приближающейся аварии. Этот вопрос касается не только людей, находящихся на отдалённом расстоянии от средств оповещения, а также граждан, страдающих недостатком слуха. Успешная защита от последствий ЧС возможна при своевременном получении или доведении сигналов оповещения ГЗ. Поэтому возникает потребность в более быстром и качественном способе информирования.

После распада Советского Союза вопросу оповещения граждан не уделяется никакого внимания, а если и имеется об этом упоминание, то только в виде измененных общесоюзных рекомендаций. Проведенный анализ нормативной литературы и законодательных актов разных стран показал [2 – 5], что схема оповещения населения осуществляется следующим образом. Оперативный дежурный центральной диспетчерской службы через соответствующие дежурные (дежурно-диспетчерские) службы осуществляет информирование об опасности с использованием: радиотрансляционных узлов; радиовещательных и телевизионных компаний; уличных городских и ведом-

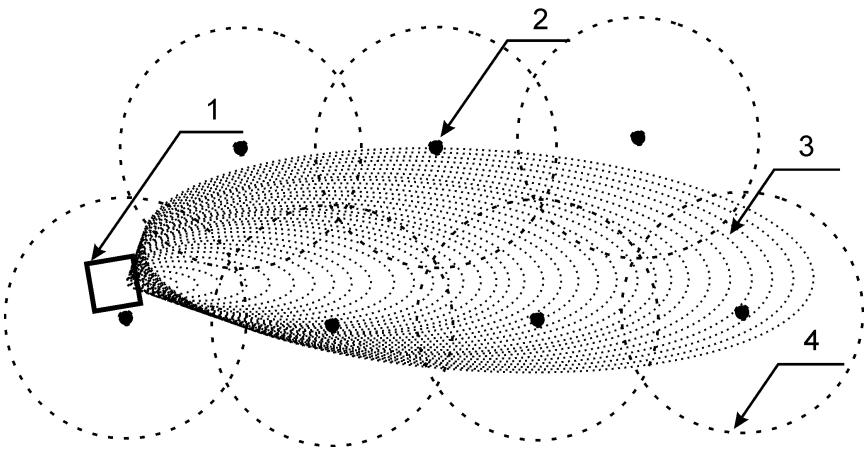
ственных громкоговорителей; электрических сирен и мегафонов; локальных систем оповещения организаций. Данная система не позволяет оперативно оповещать граждан при появлении или угрозе ЧС. При этом нет никакой гарантии, что оповещенные будут знать каким образом и в какой последовательности необходимо действовать во время надвигающейся угрозы.

Следует разработать новый способ оповещения, позволяющий в кратчайшие сроки оповестить население о возникшей угрозе (химического, биологического, военного или же социального характера), а также в нем должны сочетаться простота реализации приемов и эффективность оповещения.

Ещё издавна, когда где-то случалась беда или кому-то угрожала опасность, народ, услышав звоны или набат, собирался, узнавал о случившемся и принимал решение, как именно бороться с угрожающей опасностью. Так и теперь, нельзя оставлять людей в незнании, они должны знать обстановку, и только тогда можно рассчитывать на умные и сознательные действия, бороться с паникой и другими отрицательными явлениями. Это сохранит жизнь многим тысячам людей. Поэтому в конце 1988 года был пересмотрен и изменен порядок оповещения населения в ЧС. Продолжительное время в ГЗ применялся такой сигнал, как звук сирены. Завывающие, прерывистые гудки предприятий, транспортных средств означают новый предупредительный сигнал оповещения ГЗ "Внимание всем!" (а не "Воздушная тревога!"). В таком случае население должно было немедленно оставить свои квартиры, рабочие места, транспортные средства и укрыться в защитных сооружениях. В реальности же (при плановом или внезапном срабатывании территориальных систем оповещения) реакция людей была разная. Одни не обращали на звук внимания, другие терялись и не знали, что делать. Руководители предприятий начинали звонить по телефону в территориальные органы управления ГЗ и уточнять, что произошло, вместо того, чтобы дать команду на укрытие людей в защитных сооружениях. Не было сигналов о стихийном бедствии, которое приближается, об аварии. Возникает вопрос о том, каким образом в случае опасности можно быстро оповестить людей, где бы они не находились. Решение видится в привлечении новых технологий.

На протяжении последних 10 лет в массы активно продвигаются мобильные технологии, которые позволяют общаться в зоне действия сети. По последним данным некоторые операторы сотовой связи имеют покрытие свыше 95% территории нашей страны, а оставшиеся непокрытые сетью участки – это незаселенная местность (леса, горы). Это позволяет постоянно поддерживать связь между абонентами. У мобильных компаний, кроме мобильных переговоров, существует сервис мгновенных сообщений, в виде СМС и ММС. Они используются не только для общения абонентов, но и для рекламных и информационных целей компаниями, оказывающими этот сервис.

Предлагается использовать данный сервис для информирования населения о возникшей ЧС или угрозе её возникновения. Такими угрозами могут быть крупные пожары, выбросы СДЯВ, радиационное заражение, землетрясение, затопление, лавины и др. Рассмотрим ситуацию на примере распространения СДЯВ при аварии на химическом предприятии (рис. 1).



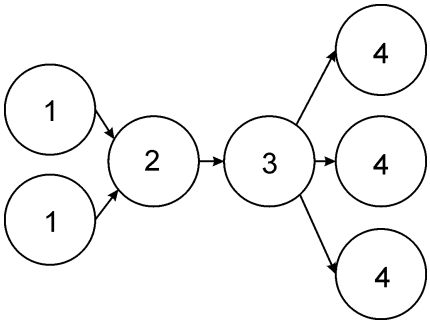
Условные обозначения:

1 – предприятие, на котором возникла авария с выбросом СДЯВ; 2 – антенна сотовой связи; 3 – распространившееся облако СДЯВ; 4 – радиус действия антенны сотовой связи.

Рис. 1. **Зона покрытия сотовой сети в зараженной местности**

Из рис. 1 видно, что для оповещения абонентов антенны сотовой связи будут использоваться адресно, то есть только в районе заражения или прогнозируемого распространения угрозы.

Предполагается, что схема передачи информации будет осуществляться следующим образом. Звонки от очевидцев аварии поступают в дежурную службу подразделения МЧС (также возможно получение информации при срабатывании автоматической сигнализации), затем производится анализ ситуации, подтверждение данных, прогнозирование распространения облака. После этого подготовленное сообщение передаётся оператору сотовой связи, после чего оператор отсылает сообщение всем абонентам в зараженной местности (рис. 2).



Условные обозначения:
1 – очевидец аварии или автоматическая сигнализация; 2 – оперативный дежурный МЧС; 3 – сотовый оператор, осуществляющий рассылку сообщений; 4 – абоненты сети, находящиеся в зараженной местности.

Рис. 2. **Схема информирования населения**

Из схемы видно, что простота передачи информации конечному получателю даст возможность не только быстро, но и точно доставить информацию.

Предполагается, что данный способ позволит не только повысить оперативность информирования, но также увеличить число оповещенных лиц, так как мобильные средства связи обширно вошли в повседневную жизнь каждого человека. Инструкции в виде текстовых или мультимедийных сообщений, полученных абонентом, позволят выполнять рекомендации по защите жизни и имущества человека, что даст возможность спасти самое дорогое – жизнь человека.

Литература: 1. Закон України "Про правові засади цивільного захисту" від 24 червня 2004 року №1859-IV // www.rada.gov.ua. 2. Постанова КМУ від 15 лютого 1999 р. №192 "Про затвердження Положення про організацію оповіщення і зв'язку у надзвичайних ситуаціях" // www.rada.gov.ua. 3. Приказ МЧС РФ №422, Мининформсвязи РФ №90, Минкультуры РФ №376 от 25.07.2006 г. "Об утверждении положения о системах оповещения населения". (Зарегистрировано в Минюсте РФ 12.09.2006 №8232). 4. Закон РФ от 21.12.1994 г. №68-ФЗ "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера". 5. Соколов Ю. И. Оповещение населения при чрезвычайных ситуациях / Под ред. В. А. Владимирова. — М.: КРУК, 2001. — 192 с.

Живко З. Б.

Живко М. О.

Войтович Ю. В.

УДК 338.65.011+330.1155

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЛІЦЕНЗУВАННЯ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ В ОВС ЯК НАПРЯМОК ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Становлення України як суверенної і незалежної держави спричинило радикальні зміни у сфері економічних відносин. Прийняття законів України "Про підприємства" та "Про підприємництво" стало підґрунтям масового розвитку підприємництва в Україні [1; 2]. Підприємництво сьогодні є однією з основних форм господарювання. Підприємницька ініціатива в умовах формування ринкової економіки стає джерелом підвищення добробуту громадян, але ефективність її здійснення за-

лежить не лише від здібностей, фінансових можливостей підприємця, а й від роботи органів виконавчої влади всіх рівнів та належного інформаційного й нормативно-правового забезпечення реалізації цих процесів.

Проблематика дослідження ліцензування полягає в тому, що в теоретичних надбаннях цьому інститутові, тим більше його інформаційному забезпеченню, приділялася недостатня увага.

Одним із найважливіших завдань у напрямку застосування ліцензій, винаходів, міжгалузевої інформації, ноу-хау та впливу їх на безпеку як підприємницької діяльності, так і держави загалом є посилення міжнародної конкуренції, створення технологічних парків, забезпечення сталого розвитку й прибутковості підприємств від упровадження стандартизації та уніфікації продукції, зміни технологій виробництва сучасних підприємств згідно з міжнародними вимогами, забезпечення екологічної безпеки виробництва.

Ця проблематика на сьогоднішньому рівні актуальна, залишається відкритою та недостатньо дослідженою.

Розглядаючи підприємництво як соціально-виробниче явище, слід зазначити, що воно, крім позитивних, має низку негативних аспектів. Насамперед, це пов'язано з тією потенційною небезпекою, що містить підприємницька діяльність, пов'язана з предметами, винаходами, їх апробацією і відносинами, які наділені особливим правовим статусом, захистом інформації щодо цих винаходів. Під небезпекою слід розуміти об'єктивно існуючу можливість негативного впливу на навколишнє середовище, екологічну систему та соціальний організм, у результаті якого їм можуть бути заподіяні якісь збитки, шкода, втрати, що погіршують їх стан чи надають їх розвиткові небажану динаміку або негативно змінюють параметри.

Ліцензування регулюють Господарський кодекс України від 16 січня 2003 р., Закон України "Про ліцензування певних видів господарської діяльності" за станом на 27 жовтня 2006 р., про внесення змін до Закону України "Про ліцензування певних видів господарської діяльності", прийнятий 27 квітня 2007 р. №994, а також інші нормативно-правові акти, що враховують особливості ліцензування конкретних видів діяльності [3 – 8]. Однак в економіко-правовому регулюванні ліцензування, захисті інформаційного простору ліцензування недостатня системність, є недоліки, які вказують на необхідність комплексного наукового дослідження проблем ліцензування, його інформаційного забезпечення та економіко-правової основи.

Розвиток ідей щодо обґрунтування поняття ліцензування та підстав його здійснення знайшов своє відображення в роботах В. Авер'янова, Ю. Битяка, С. Вітвицького, З. Гладуна, Л. Савченко, Н. Саніахметової, О. Шеваріхіна, Ю. Шемшученка, В. Шкарупи та інших учених. Окремі правові аспекти ліцензування розроблені в науково-теоретичних дослідженнях, зокрема, в роботах А. П. Альохіна, Е. Е. Бекерової, І. І. Єремєєнко, А. П. Герасимова, А. В. Губанова, Р. І. Денисова, Л. В. Шестак. Науковими дослідженнями питань обґрунтування впроваджень і використання підприємствами інновацій та інтелектуальних ресурсів займалися Г. Андрощук, В. Геєць, О. Лищишин, Є. Крикавський, І. Михасюк, Л. Петрович, І. Тивончук, А. Шеваріхін, В. Яцкова та ін.

Питання щодо економіко-правових аспектів ліцензування розглядалися в нашій державі частково, з позицій відомчого регулювання та з урахуванням місця ліцензування серед схожих правових режимів. Тож мета даної статті – доопрацювання принципів державної політики у сфері ліцензування та правового статусу органів, що здійснюють її реалізацію, зокрема органів внутрішніх справ, та аналіз процедури ліцензування, визначення її етапів.

Наукові дослідження в напрямку застосування ліцензій, винаходів, міжгалузевої інформації в розвитку підприємництва є одним із головних завдань. У сучасному світі ліцензії, ноу-хау міжгалузева інформація зараховується до інтелектуальної власності. Свої витоки патентне законодавство бере з XVI століття у Великобританії, Франції та США. До наших часів дійшла патентна система, яка започаткована у Німеччині з кінця XIX століття.

Ліцензування як форма державного обмеження підприємницької ініціативи не є винаходом сьогодення. Однією з перших спроб державного регулювання підприємницьких відносин можна вважати надання в деяких країнах (Англія, Франція, Росія тощо) на початку XIX століття "ліценців" або "пільгових листів", тобто грамот, що давали власникам суден право ввозу і вивозу заборонених товарів за часів континентальної системи. У вигляді нагляду чи інспекції таке державне регулювання набуло певного розвитку в XIX столітті у багатьох країнах. Урядовий нагляд щодо мануфактур, у яких крилася будь-яка небезпека — пожежна, санітарна, економічна, кримінальна, соціальна, — в більшості країн існував у двох головних формах: 1) законодавство, забезпечуючи кожному право вільного створення фабричного або ремісничого закладу і вимагаючи від засновника лише замовлення, зобов'язувало мануфактуру, що визнавалась небезпечною, отримувати попередній дозвіл уряду, враховуючи ймовірність відмови у наданні цього дозволу; 2) стосовно окремих мануфактур уряд мав право постійного нагляду як за допомогою своїх урядових інспекторів, так і іншими способами згідно з чинними законами. Особливий пік розвитку патентування відзначається у XX столітті, коли третина людської інтелектуальної праці припала на створення винаходів, ноу-хау, ліцензій та міжгалузевої інформації.

За російським правом, мануфактури за порядком їх відкриття поділялися на категорії: 1) визнані нешкідливими, які могли створюватися у будь-якому місті; 2) ті, заснування яких не потребувало дозволу влади загального управління, але вимагався дозвіл міністерства внутрішніх справ або міністерства фінансів; 3) створення яких заборонялося законом [9 – 11].

За деякими джерелами економічна категорія "ліцензія" походить від італійського "*lizentia*" – дозвіл [12, с. 12]. В економічній літературі є різні визначення поняття "ліцензія". Зокрема, за укла-

деним авторами словником, виокремлено такі визначення: 1) дозвіл, що видається власником (ліцензіаром) патенту, винаходу, торгової марки і т. п. іншій особі або фірмі (ліцензіату) на його промислове та комерційне використання на умовах, передбачених ліцензійною угодою; 2) дозвіл, що видається державою юридичним і фізичним особам на право певної господарської діяльності; 3) дозвіл на зовнішньоекономічну діяльність, який видається державою; 4) дозвіл, що видається державними органами юридичним та фізичним особам на право певних видів суспільно корисної діяльності, в тому числі зовнішньоекономічної, використання нематеріальних ресурсів протягом певного терміну за обумовлену винагороду [13, с. 189].

Інтелектуальна власність зрідка є предметом ліцензійного договору. Ліцензія – це техніко-економічний проект, у який входять винаходи, промислові зразки, ноу-хау, міжгалузева інформація, корисні моделі, товарні знаки, внаслідок реалізації яких власник отримує прибуток.

На думку авторів, особливо пильній увазі ліцензування підпадає вид підприємницької діяльності, що підпадає під юрисдикцію МВС, на якій зупинимось конкретніше.

Серед органів виконавчої влади, що безпосередньо здійснюють ліцензування підприємницької діяльності, важливу роль відіграють органи внутрішніх справ (ОВС), на які покладено повноваження щодо ліцензування таких видів підприємництва: 1) виготовлення й реалізація спеціальних засобів, заряджених речовинами сльозоточивої та дратівливої дії, індивідуального захисту, активної оборони та засобів для виконання спеціальних операцій і оперативно-розшукових заходів; 2) виробництво, ремонт і реалізація спортивної, мисливської вогнепальної зброї та боєприпасів до неї, а також холодної зброї, пневматичної зброї калібру понад 4,5 мм і швидкістю польоту кулі понад 100 м/з; 3) створення та утримання стрілецьких тирів, стрільбищ, мисливських стендів; 4) надання послуг, пов'язаних з охороною власності, а також охороною громадян; 5) надання послуг ВГІРФО щодо оформлення паспортів громадянина України, паспортів громадянина України для виїзду за кордон, проїзного документа дитини, реєстрації місця проживання тощо; 6) надання послуг ДАІ, зокрема, дозволів на перевезення небезпечних вантажів, складання іспитів та видача посвідчення водія, видача дозволів і схем маршрутів транспорту та ін.; 7) довідкова інформація адресного бюро; 8) видача довідок УІТ про відсутність судимості тощо [8; 14 – 17].

Реалізація перерахованих видів підприємницької діяльності пов'язана з використанням предметів і речовин, що належать до категорії джерел підвищеної небезпеки під час забезпечення громадської безпеки. Крім того, ці види підприємництва тісно стикаються із суспільними відносинами, що входять до сфер громадської безпеки, профілактики, порядку управління, забезпечення захисту майна суб'єктів господарювання та громадян інтелектуальної власності, безпеки держави загалом.

Це обґрунтовує покладання обов'язку ліцензування зазначених видів підприємницької діяльності на органи внутрішніх справ. З цією метою Головними управліннями адміністративної служби міліції і Державної служби охорони, управлінням технічних інформацій МВС України були розроблені Інструкції про порядок видачі суб'єктам підприємницької діяльності ліцензій на право здійснення відповідних видів діяльності, Умови і правила здійснення підприємницької діяльності, Інструкція про порядок здійснення контролю за діяльністю суб'єктів підприємництва, інші документи. До штатного розкладу структур відповідних служб і підрозділів було введено співробітників, обов'язки яких доповнилися функціями щодо реалізації завдань ліцензування.

Обсяг і види заходів, що виконуються, характерний об'єкт впливу, специфічні методи діяльності – все це свідчить про становлення нового самостійного напрямку адміністративної діяльності органів внутрішніх справ, спрямованого на ліцензування окремих видів підприємництва.

Проблемними питаннями у цій сфері вважаємо: 1) діяльність органів внутрішніх справ з ліцензування підприємницької діяльності фактично не має правової регламентації, у Законі України "Про міліцію" про це навіть не згадується; 2) відомчими нормативними актами не передбачено регламентації ліцензійної діяльності; 3) відсутня внутрішньосистемна взаємодія кадрового, матеріально-технічного забезпечення зі статусом і правовим положенням ліцензійної роботи; 4) відсутня системність ліцензійної діяльності; 5) не розроблена модель служби ліцензійної роботи; 6) не визначене місце ліцензійної служби в структурі ОВС; 7) не розроблені нормативні акти, що регламентують діяльність ліцензійної служби; 8) не ведеться статистична звітність за видами ліцензування; 9) не об'єднано в єдину систему окремі види ліцензійної роботи в ОВС; 10) не вирішена загальна проблема здійснення ліцензійної роботи органами внутрішніх справ.

Таке становище з ліцензійної діяльності веде до зниження ефективності та результативності роботи, відсутності контролю й належного ставлення до важливості інституту ліцензування з боку керівного складу, виникнення штучних бар'єрів при здійсненні взаємодії з іншими службами і підрозділами органів внутрішніх справ.

Отже, вимоги до співробітника ОВС, який здійснює роботу з ліцензування окремих видів підприємницької діяльності: повинен мати юридично-економічну освіту (як мінімум необхідно закінчити факультет економічної безпеки ВНЗ МВС); впевнено орієнтуватися в правових актах, що регламентують питання здійснення підприємницької діяльності та її ліцензування; мати необхідний мінімум знань в економічних, фінансових, бухгалтерських і технічних питаннях, обсяг та спрямованість яких залежать від виду підприємницької діяльності, ліцензування якої здійснюється; мати навички професійної психології та відповідати критеріям професійної етики; самостійно поглиблювати й розширювати знання, вдосконалювати навички, що необхідні в роботі.

Іншою важливою проблемою в організаційно-управлінській діяльності органів внутрішніх справ щодо ліцензійної роботи є питання матеріально-технічного забезпечення. Найбільш гостро

відчувається недостатня кількість організаційної і комп'ютерної техніки, комп'ютерного програмного забезпечення. Комп'ютерна техніка та програмне забезпечення, які використовуються органами ліцензування ОВС, морально та фізично застарілі.

Не менш важливою проблемою ліцензування в ОВС є взаємодія різноманітних служб. Адже під час здійснення ліцензування підприємницької діяльності інспектори з ліцензійної роботи постійно контактують із співробітниками підрозділів служб боротьби з економічною злочинністю, боротьби з організованою злочинністю, адміністративної служби міліції та інших служб органів внутрішніх справ, направляючи їм відповідні запити. Матеріали щодо видачі ліцензій не можуть бути оформленими (протягом 20 днів) через відсутність результатів перевірок відповідних служб, що спричиняє порушення термінів видачі ліцензій, знижує якість матеріалів, спонукає підприємців до вишукування шляхів терміного вирішення питання та матеріальних і моральних збитків.

Необхідність і об'єктивний характер інституту ліцензування підприємницької діяльності, підвищену громадську небезпеку видів підприємництва, ліцензування яких покладено на органи внутрішніх справ, наявні прогалини в правовому регулюванні та організації діяльності органів внутрішніх справ щодо ліцензування підприємництва потребують ще вивчення, впорядкування та економіко-правового дослідження цього важливого інституту.

Література: 1. Закон України "Про підприємництво" // Відомості Верховної Ради. – 1991. – №14. – 168 с. 2. Закон України "Про підприємства" // Відомості Верховної Ради (ВВР). – 1991. – №24. – 272 с. 3. Господарський кодекс України // Офіційний вісник України. – 2003. – №11. 4. Закон України "Про внесення змін до Закону України "Про ліцензування певних видів господарської діяльності": Прийнятий 27 квітня 2007 р. №994 // Урядовий кур'єр. – 2007. – 14 червня. – (№104). – С.18. 5. Закон України "Про ліцензування певних видів господарської діяльності". За станом на 27 жовтня 2006 р. – К.: Парлам. вид., 2006. – С. 29. 6. Ліцензійні умови провадження господарської діяльності з виробництва, ремонту вогнепальної зброї та боєприпасів до неї, холодної зброї, пневматичної зброї калібру понад 4,5 міліметра і швидкістю польоту кулі понад 100 метрів на секунду, торгівлі вогнепальною зброєю та боєприпасами до неї, холодною зброєю, пневматичною зброєю калібру понад 4,5 міліметра і швидкістю польоту кулі понад 100 метрів на секунду. Затверджено наказом Державного комітету України з питань регуляторної політики та підприємництва, Міністерства внутрішніх справ України №53/213 від 21 березня 2001 р. // Офіційний вісник України. – 2001. – №14. – 20 квітня. 7. Ліцензійні умови провадження господарської діяльності з виробництва спеціальних засобів, заряджених речовинами сльозоточивої та дратівної дії, індивідуального захисту, активної оборони. Затверджено наказом Державного комітету України з питань регуляторної політики та підприємництва, Міністерства внутрішніх справ України №53/213 від 21 березня 2001 р. // Офіційний вісник України. – 2001. – №14. 8. Постанова Кабінету Міністрів України "Про затвердження переліку органів ліцензування" №1698 від 14 листопада 2000 року // Урядовий кур'єр. – 2000. – №228. – 7 грудня. 9. Законы о частной фабрично-заводской промышленности / Под ред. Д. И. Гутцайт. – М., 1913. – С. 79. 10. Антонович А. Я. Курс государственного благоустройства (полицейского права). – К., 1890. – Ч. 2. – С. 117. 11. Шеварихін А. О. Ліцензування підприємницької діяльності: історія та сучасність // http://www. naiau. kiev. ua/tslc/pages/biblio/visnik/. 12. Лищишин О. І. Можливості управління науково-технічним прогресом за допомогою винаходів, ліцензій, ноу-хау і міжгалузевої інформації. Монографія. – Львів: Бібльос, 2006. – 300 с. 13. Живко З. Б. Словник сучасних економічних термінів / З. Б. Живко, М. О. Живко, І. Ю. Живко. – Львів: Край, 2007. – 384 с. 14. Постанова Кабінету Міністрів України "Положення про дозвільну систему" №576 від 12.10.1992 р. // Іменем Закону. – 1992. – №4. 15. Указ Президента України "Про запровадження дозвільної системи у сфері підприємницької діяльності" від 13 серпня 2002 року // Офіційний вісник України. – 2002. – №33. 16. Указ Президента України "Про запровадження єдиної державної регуляторної політики у сфері підприємництва" від 22 січня 2000 року // Офіційний вісник України. – 2000. – №4. 17. Положення про Міністерство внутрішніх справ України. Затверджено Указом Президента України від 17 жовтня 2000 року // Офіційний вісник України. – 2000. – №42. 18. Декларація про державний суверенітет України // Відомості Верховної Ради. – 1990. – №31. – С. 429. 19. Конституція України // Відомості Верховної Ради. – 1996. – №30. – С. 141. 20. Європейська Конвенція з прав людини, підписана 9.11.1995 р. // http://www. coe. kiev. ua/. 21. Закон України "Про патентування деяких видів підприємницької діяльності" // Відомості Верховної Ради. – 1996. – №20. – С. 82. 22. Закон України "Про міліцію" // Відомості Верховної Ради. – 1991. – №4. – С. 20. 23. Закон України "Про охорону прав на винаходи і корисні моделі" (із змінами і доповненнями, внесеними Законом України №35, 2003) // www.rada.gov.ua. 24. Бекирова Э. Э. Правовое регулирование лицензирования определенных видов хозяйственной деятельности. Диссертация на соискание научной степени кандидата юридических наук. – Донецк: Институт экономико-правовых исследований НАН Украины, 2006. 25. Бекірова Е. Е. Процедура ліцензування певних видів господарської діяльності // Підприємництво, господарство і право. – 2005. – №6. – С. 85 – 88. 26. Гаращук В. Контроль та нагляд у державному управлінні: порівняльна характеристика // Виконавча влада і адміністративне право. – К.: Ін-Юре, 2002. – С. 453 – 460. 27. Шамрай І. А. Правові основи створення фінансових установ в Україні та ліцензування їх операцій. Автореф. дис. ... канд. юрид. наук. – К.: НАН України, Інститут держави і права ім. В. М. Корецького, 2007. – 20 с. 28. Закон України "Про лікарські засоби" // Відомості Верховної Ради. – 1996. – №22. – Ст. 86 (із змінами і доповненнями, внесеними Законом України №3370-IV (3370-15) від 19.01.2006) // http://zakon. rada. gov. ua/.

Лукацкий А. В.

УДК 681.3

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. УДОБСТВО И ПРАКТИЧНОСТЬ

Установив систему защиты, не ждите благоприятных отзывов
от пользователей.
Законы Мерфи для информационной безопасности

Постоянно приходится слышать мнения о том, что безопасность – это сложно и неудобно. Последнее и вызывает основные проблемы с повсеместным внедрением систем защиты. Во многих книгах можно прочесть о том, что, занимаясь безопасностью, нужно соблюдать баланс между удобством и защищенностью. Нельзя создать бронированный автомобиль, который ездит как Ferrari. Нельзя защитить свое жилище, не возведя вокруг него высоких стен или не установив на окнах решеток, которые мешают любоваться красотами. Нельзя построить денежное хранилище и открыть доступ к нему всем желающим. Но… стремиться к компромиссу необходимо обязательно. Более того, современные технологии позволяют сделать то, что раньше было невозможно представить. Например, объединение карты доступа в помещения и токена для доступа к компьютеру. Теперь это возможно, что сразу сняло множество проблем с забыванием одной из карт дома, путаницей с этими картами на входе в здании и создании очередей из-за этого и т. д.

Смежная безопасность и удобство – внедряя систему безопасности, нельзя забывать о том, что не она является самоцелью (хотя для многих специалистов по защите это именно так). Безопасность, если мы не говорим об отдельных сферах нашей жизни, носит второстепенный характер. Однако это не умаляет ее важности. Как же разрешить этот конфликт интересов и можно ли вообще это сделать? Как показывает практика – можно. Возьмем 2 примера – положительный и отрицательный. Начнем с последнего, как наиболее близкого по времени.

Предотвращенный теракт в Великобритании. После ареста террористов в аэропортах по всему миру были введены "драконовские" меры к пассажирам – "для их безопасности". Любые жидкости были запрещены для провоза в ручной клади; электроника тоже. Сильно ли это подняло безопасность? Не знаю. Но вот проблем доставило много. Во-первых, запрет на провоз жидкостей снизит доходы магазинов Duty Free. Во-вторых, запрет на перевозку лэптопов и КПК мог "убить" сегмент бизнес-перевозок, так как путешествующие бизнес-классом бизнесмены врядли с энтузиазмом отнесутся к многочасовым полетам без своих инструментов ведения бизнеса. В-третьих, как быть с теми, кому жидкость нужна "по определению". Например, для хранения контактных линз. А если мне нужно лекарство, которое продается без рецепта, но от этого оно не становится менее важным для меня. И это не говоря про многочасовые очереди в аэропортах на пунктах досмотра, отказ от полетов, сдача купленных билетов, ущерб репутации, недовольство клиентов и т. д. Выиграли от этого, пожалуй, только компании, занимающиеся железнодорожными перевозками. И все это ради безопасности. Со временем все встало на свои места. Большинство запретов было снято под давлением общественности. Проносить в салон самолеты лэптопы, напитки Duty Free и т. д. все-таки разрешили [1].

У данной проблемы есть и другая сторона. Лишний раз было продемонстрировано, что только реактивный подход к безопасности неэффективен. Неужели, достигнув своей цели, террористы захотят немедленно повторить свой "успех"? Вряд ли. В этом случае теряется эффект "нагнетания страха", а именно он является движущей силой терроризма. Возникает парадокс. Преступление произошло, а меры по его предотвращению принимаются после, а не до. Неужели спецслужбы не знали о жидкой взрывчатке? Неужели никто не думал, что электронные приборы могут выступать в качестве детонатора? Знали, но действовали по принципу "пока гром не грянет…" В итоге введенные меры существенно ухудшили отношение простых граждан к безопасности.

Теперь посмотрим на другую область, в которой также невозможно обойтись без безопасности, – автомобилестроение. Здесь производители демонстрируют совершенно иное отношение к вопросам защиты водителей и пассажиров. Возьмем хороший автомобиль, сядем за руль и тронемся с места. Нарастающий сигнал предупредит вас о том, что вы и ваши пассажиры не пристегнуты. Вы можете проигнорировать сигнал, и он через некоторое время отключится, но всю вину за возможное ДТП вы будете уже нести сами – ведь "железный друг" вас предупреждал. Вы начинаете движение и постепенно увеличиваете скорость. Попав на скользкий участок или крутой поворот вы даже не чувствуете, как вас заносит или "уводит" в сторону – незаметно работает система курсовой устойчивости, антиблокировочная система и множество других полезных и невидимых подсистем. Сталкиваетесь ли вы с системами безопасности автомобиля? Практически нет. Видимое проявление происходит только в минуту опасности. В крайнем случае срабатывают подушки безопасности, уберегая вас от серьезных повреждений. В некоторых моделях автомобилей дошло до того, что они оснащаются ограничителями максимальной скорости (даже если машина может и

больше) и алкотестерами (мотор не заработает, если в салоне будет "чувствоваться" запах спиртных напитков).

Налицо два подхода к безопасности клиента. В первом случае безопасность ставится во главу угла и только мешает; во втором – все наоборот. Мне по душе второй подход. Именно так необходимо внедрять защитные решения – они должны максимально эффективно решать свои задачи, не мешая при этом выполнению основных бизнес-функций.

Психологическая приемлемость. 30 лет назад, еще в 1975 году Джером Зальтцер и Майкл Шредер определили "психологическую приемлемость" (psychological acceptability), как один из 8 ключевых принципов при построении защищенных систем. Звучит он следующим образом: "Очень важно, чтобы интерфейс взаимодействия с пользователем был удобным в использовании; чтобы пользователи запросто и "на автомате" использовали механизмы защиты правильным образом. Если образ защиты в уме пользователя будет соответствовать тем механизмам, которые он использует на практике, то ошибки будут минимизированы. Если же пользователь должен переводить представляемый им образ на совершенно иной "язык", он обязательно будет делать ошибки". Суть этого принципа проста – механизм безопасности не должен делать доступ к ресурсу или иное действие более сложным, чем если бы этого механизма не было. Иными словами, на практике это означает, что безопасность должна вносить лишь незначительную сложность в защищаемые операции [1].

Однако на практике этот принцип почти не соблюдается – интерфейс многих систем защиты хоть и рекламируется как "интуитивно понятный", но проектируется без учета требований к эргономике, практичности, удобству и простоте использования. А это подчас бывает гораздо важнее, чем криптостойкость, использование двухфакторной аутентификации, эвристических алгоритмов для обнаружения вредоносных программ и т. п. Информационные системы становятся все более сложными и громоздкими, а значит возрастает вероятность совершить ошибку и неправильно сконфигурировать, эксплуатировать, обновить или поддерживать защищаемую систему. Иными словами, безопасность ослабевает.

Разумеется, воплотить на практике этот принцип не так то просто. Уж слишком много участников в жизненном цикле системы защиты, начиная от программиста и заканчивая самим пользователем. Реализовывать этот принцип надо в расчете на тех, кто будет использовать систему, а не тех, кто ее создает. Это простое правило известно по многим другим отраслям. Например, в маркетинге есть классический принцип – "прежде чем выпускать на рынок новый продукт, встань на место его потребителя и подумай, нужен ли ему такой продукт". В безопасности необходимо делать то же самое – рассчитывать надо не на сотрудника отдела системы защиты и даже не на среднестатистического пользователя. Исходить надо из худшего, то есть в расчете на самого "тупого" потребителя. В противном случае останется только вспомнить законы Мерфи для информационной безопасности: "Если вы уверены, что написанная вами инструкция по правилам выбора паролей не может быть понята неправильно, всегда найдется сотрудник, который поймет ее именно так" [2]. На практике же разработчики систем защиты создают свои продукты "для себя", исходя из своих собственных представлений и ожиданий. Хотя и эти представления могут сильно отличаться в зависимости от того, где они работают – одно дело компания Cisco или Microsoft со своими законами и налаженным процессом разработки и совсем другое – небольшая российская компания-стартап с 5 – 10 программистами.

Целью статьи является наглядный показ механизма реализации удобства и практичности информационной безопасности.

Возьмем самый распространенный защитный механизм, с которым сталкивается каждый пользователь чуть ли не ежедневно. Речь пойдет о паролях. Классическая рекомендация, с которой сталкивается любой неискушенный человек, – выбирайте пароли так, чтобы они не содержали известных слов или комбинаций цифр (номер паспорта, телефон, день рождения), состояли из символов в обоих регистрах, также включали цифры и знаки препинания. А еще необходимо, чтобы пароль был не менее 8 символов. В итоге мы регулярно сталкиваемся с такими паролями, как например, 8HguJ7hY. С точки зрения безопасности он почти идеален, но вот запомнить его практически нереально. А если учесть, что таких паролей пользователь может иметь несколько (для компьютера, для Интернета, для коммуникатора, для базы данных, для ключевых приложений и т. д.), то в результате пользователь запишет его или их на бумажке или сохранит в текстовом файле на своем компьютере. Если же отдать выбор пароля на откуп пользователю, то он выберет что-нибудь тривиальное. Не буду приводить результатов различных исследований, но ситуация с самостоятельным выбором действительно удручающая.

Это то, с чем нам приходится сталкиваться постоянно. Поставив во главу угла безопасность и, забыв про принцип психологической приемлемости, мы получаем огромное количество проблем – утерянные или легко угадываемые пароли. Разработчики просто не думают, что можно сделать что-то более эффективное. Например, графические пароли, которые не менее эффективны, но более удобны, чем обычные сложно запоминаемые последовательности символов. Но используется такой способ представления пароля редко, хотя в современных графических системах нет особых проблем в реализации этого механизма (у меня на коммуникаторе, например, реализован именно такой механизм).

Если же вспомнить про принцип психологической приемлемости, то один из путей его реализации – парольные брелки или токены, которые хранят все пароли к разным системам. Пользователю надо знать только главный пароль к брелку. И хотя мы существенно облегчаем жизнь пользователю, это только видимое решение проблемы. Но что делать, если он забудет главный пароль или злоумышленник сможет этот главный пароль подобрать? Конечно существуют системы

централизованного управления токенами, но они внедряются не везде и тоже имеют свои ограничения. Зато гораздо более эффективна с точки зрения названного принципа биометрия, так как пользователю не надо помнить пароли и злоумышленнику не так просто выдать себя за другого человека. К сожалению, разработчики часто идут по пути наименьшего сопротивления и поэтому биометрическая аутентификация пока редкость, несмотря на наличие достаточно эффективных алгоритмов и практических решений.

Хотя и на обычных паролях также можно реализовать достаточно эффективную систему. Например, SofToken (рис. 1). На экране мы видим, что пользователю дается всего две кнопки "Get Password" и "Close". Вторая закрывает приложение, а первая генерит одноразовый пароль, который даже не надо специально копировать в буфер обмена – все делает система. Вам достаточно ввести созданный пароль в какое-нибудь приложение и пройти процесс аутентификации [3].

Рис. 1. **Система генерации одноразовых паролей**

В качестве такого приложения может быть назван, например, VPN-клиент компании Cisco (рис. 2). В данном примере мы должны произвести всего два действия – выбрать VPN-шлюз, через который будем подключаться к корпоративной сети, и ввести аутентификационные параметры. В зависимости от настроек первый этап можно опустить. Например, у нас всего одна точка подключения к корпорации или шлюз выбирается автоматически. В этом случае достаточно ввести только пароль пользователя, который может быть сгенерирован программой SofToken. Можно заметить, что в обоих приложениях имя пользователя уже введено и пользователя не заставляют делать это каждый раз, повышая риск сделать ошибку в имени, тем самым увеличив время на вход в систему или вызвав раздражение пользователя.

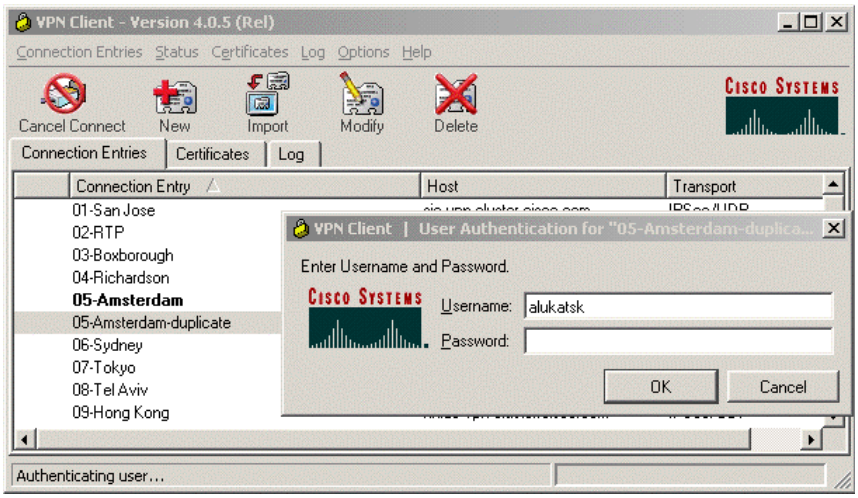


Рис. 2. **VPN-клиент Cisco**

Интегрировав VPN-клиент Cisco с токеном (например, от компании Aladdin) мы исключаем и этап ввода пароля, который берется автоматически из токена.

Другой пример – патчи и системные обновления. К сожалению, программное обеспечение не совершенно, как и люди, его создающие. А значит обновления, устраняющие те или иные уязвимости или ошибки, нам будут нужны всегда. Принцип психологической приемлемости применительно к патчам означает, что они должны устанавливаться прозрачно для пользователя и системного администратора. Пока же на практике это происходит не всегда, хотя многие производители систем управления патчами уже на полпути к решению этой проблемы. Например, есть в компании все патчи и ПО распространяются и устанавливаются централизованно с помощью решений компании Altiris, то это происходит абсолютно прозрачно для пользователей. Даже инсталляция такой системы защиты, как Cisco Security Agent на 47000 лэптопов по всему миру произошла абсолютно прозрачно и без участия пользователей в этом процессе.

Исходя из проведенных исследований, можно сделать вывод, что современный мир диктует нам свои условия – без безопасности нам уже не обойтись. И у нас остается два пути – оставить все как есть или попробовать реализовывать принцип психологической приемлемости. Безопасность – это не только какие-то механизмы или алгоритмы. Это продукт, включающий также и другие компоненты, такие, как человеческий фактор и различные правила и политики. Игнорирование или недооценка любого из этих факторов приводит к неудаче.

Безопасность очень тесно связана с человеческим фактором. Даже лучшие политики безопасности или методы защиты могут быть разрушены или обойдены, если пользователь найдет их сложными в реализации или "мешающими жизни". Поэтому, прежде чем пускать ту или иную систему в "свободное плавание", необходимо проверить ее на следование принципу психологической приемлемости. Тестирование на пользователях – вот обязательное условие его реализации. Недостаточно проверить систему на программистах или сотрудниках отдела тестирования. Нужно привлечь тех, кто затем будет использовать эту систему. Только в этом случае мы можем быть уверенными, что система будет не только безопасной, но и удобной. Будьте как злоумышленники, которые обращают больше внимания на человеческий фактор, чем разработчики средств защиты (достаточно вспомнить действия Кевина Митника и многих других хакеров, применяющих социальный инжиниринг).

Хотя конечно надо понимать, что реализация принципа психологической приемлемости может обойтись дороже, чем отказ от него и следование стандартной практике создания защищенных систем. Возможно, это тоже является препятствием на пути повсеместного внедрения принципов создания эргономичных систем защиты. Ведь любой разработчик системы безопасности думает о рентабельности, а любые дополнительные шаги (особенно тестирование) не только ее снижают, но и увеличивают время вывода продукта на рынок с жестокой конкуренцией.

В качестве дальнейшего развития данного вопроса можно предложить, что со временем разработчики систем защиты поймут свою ошибку и начнут уделять внимание не только самым современным алгоритмам и методам безопасности, но и такой "простой" теме, как удобство и практичность.

Литература: 1. http://www. ischool. berkeley. edu/~rachna/security_usability. html – набор ссылок на различные публикации об удобстве и безопасности. 2. http://www. securitylab. ru/opinion/212050.php. 3. Security and Usability. Lorrie Faith Cranor, Simson Garfinkel. O'Reilly. 2005

УДК 657.1

Кузнецова С. А.

ПРОЦЕС ДОКУМЕНТУВАННЯ ЯК СКЛАДОВА ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ В БІЗНЕСІ

Між обліковою системою та середовищем – системою управління суб'єктами господарювання – існує зв'язок. Система управління є не тільки більш глобальною системою, а й в оточенні неї облікова система існує та функціонує. Як наголошують Ч. Хорнгрен, Дж. Фостер, Ш. Датар [1, с. 47], існування облікових систем необхідно для прийняття правильних управлінських рішень, які сприяють досягненню цілей бізнесу організації. При цьому повністю поділяємо думку зазначених учених, що в якості цілей функціонування облікових систем потрібно розглядати: створення періодичної (рутинної) внутрішньої звітності для управлінських рішень; формування нерегулярних (спеціальних) звітів для управлінських рішень; створення зовнішньої звітності, що призначена для інвесторів, органів державної власності та інших користувачів.

Ґрунтуючись на вищевикладеному, констатуємо, що передумовою та необхідністю реформування облікової системи є зміна інформаційних властивостей управління. Автор не ставить завдання розглянути всі складові організації інформаційної системи в бізнесі, оскільки це не є метою даного дослідження. Але вважаємо за необхідне приділити увагу організаційним питанням процесу документування облікової інформації з огляду на той факт, що документування виконує:

"превентивну функцію" в аспекті недопущення чи зведення до мінімуму ризику присвоєння або приховування майна суб'єктів господарювання;

доказову функцію з огляду на підтвердження фактів господарської діяльності підприємств.

Як зазначає Бетге [2, с. 43], документування є передумовою для досягнення певної системи цілей будь-якого підприємства. Професор В. М. Олійник переконаний [3, с. 61], що дослідження технологічних особливостей організації облікового процесу на підприємствах усіх форм власності забезпечить покращення якості облікової інформації, її значущості, істотності, реальності, об'єктивності та підвищить ефективність використання в ринковому середовищі.

Об'єднуючим ґрунтовним підходом, який зумовлює організацію процесу документування облікової інформації та визначає відповідні організаційні принципи в межах будь-якого суб'єкта господарювання, вважаємо синергічний підхід. Упровадження вказаного підходу зосереджує увагу на необхідності з'єднання, інтеграції окремих складових процесу документування в єдиній інформаційній системі. Безперечною перевагою синергізму є підвищення ефективності облікової інформації за кількісною та якісною ознакою внаслідок системної організації процесу її документування на всіх стадіях облікового процесу за всіма сегментами та напрямками діяльності в загальній системі управління.

Розглядаючи організацію як засіб кількісного упорядкування процесу документування облікової інформації, пропонуємо встановлювати наступні принципи.

Використання принципу синергічної єдності спрямовано на забезпечення одноразової реєстрації облікової інформації про здійснену господарську операцію в первинному бухгалтерському документі з наступним єдиним фіксуванням в облікових регістрах. Таким чином, первинний документ повинен нести в собі весь спектр облікової інформації, необхідний системі управління щодо факту господарського життя, який у ньому фіксується. При цьому реєстрації підлягає вся облікова інформація, в тому числі така, що має грошовий вимірник, і така, що вимірюється в інших одиницях (інформація про використаний робочий час – одиниця виміру: людино-годин; інформація про кількісний склад працівників підприємства – одиниця виміру: працівники (особи); інформація про час на виробництво продукції, про виробіток працівників – одиниця виміру: нормо-години; інформація про обсяги виробничих запасів – одиниця виміру: тони, літри, штуки тощо). Під час формування інформації в бухгалтерському регістрі синергічна єдність досягається шляхом виконання правила одноразової суцільної реєстрації наявної в первинному документі облікової інформації.

Принцип адаптивності передбачає, що процес документування облікової інформації повинен ґрунтуватися на структурній побудові системи управління, в межах якої він буде функціонувати. Так, у функціональній системі управління інформація документується за функціональною ознакою – за визначеними функціями системи управління; при побудові системи управління за географічною ознакою процес документування організовується в межах географічного сегмента з подальшим наданням консолідованої звітності; при функціонуванні господарчої системи управління необхідно передбачати реєстрацію та накопичення облікової інформації за господарськими сегментами й узагальнення за підприємством загалом; використання матричної структури управління потребує документування облікової інформації за визначеними сегментами з подальшим групуванням за функціональною ознакою.

Паралелізм має на увазі обов'язковість побудови та наявності процесу документування облікової інформації в усіх складових системи управління суб'єкта господарювання. Таким чином, документування виступає як документальне вираження системи дій системи управління та є підтвердженням означених дій. Виконання цього принципу досягається через розгляд організації процесу документування в якості неодмінної вимоги функціонування діючих та впровадження нових напрямків менеджменту, що забезпечує інформаційну наповненість системи управління.

Принцип терміновості спрямований на дотримання строків надання облікової інформації. Встановлення термінів надання та обробки документів дозволяє забезпечити рівномірність документування, планомірність руху документів і можливість планування облікового процесу загалом.

Послідовність побудови досягається при використанні принципу неперервності, за яким необхідно організовувати процес документування в межах певних послідовних стадій обробки облікової інформації, починаючи з її реєстрації в первинному документі та закінчуючи наданням користувачам у бухгалтерській звітності.

Прямоточність (відповідність) облікової інформації передбачає організацію руху документів відповідно до руху об'єктів обліку та конкретних функціональних потреб користувачів облікової інформації. Так, документування облікової інформації щодо руху виробничих запасів можна організовувати наступним чином:

оприбуткування виробничих запасів здійснюється на підставі прибуткової накладної;

відпуск у виробництво виробничих запасів відбувається з оформленням відповідної вимоги на відпуск;

факт виробництва напівфабрикату з використанням виробничих запасів підтверджується складанням накладної на виробництво напівфабрикату;

випуск та передача до складу готової продукції проводиться на підставі реєстрації облікової інформації в накладній на випуск готової продукції;

господарська операція з продажу готової продукції документується з використанням відповідної накладної на продаж.

Використання принципу пропорційності передбачає встановлення співвідношення між окремими елементами організаційного процесу. При цьому в якості останніх виступають:

облікова інформація з огляду на її обсяги;

кадри;

технічне та програмне забезпечення.

Виходячи з кількості первинних документів, установлюється потреба в облікових регістрах. У свою чергу, окреслені обсяги облікової інформації визначають необхідні технічні та програмні засоби забезпечення процесу її документування. Наявність останніх визначає вимоги до кадрового складу робітників, які зайняті в процесі документування облікової інформації. Доречним на цьому етапі буде враховувати притаманну залежність певних складових між собою, яка полягає в можливості зменшувати розміри та значущість одного елементу за рахунок збільшення іншого, що обумовлює відповідні структурні зміни.

Наприклад, організація процесу документування облікової інформації з використанням сучасного програмного забезпечення (в тому числі розробленого в рамках ERP-систем – Enterprise Resource Procession) скорочує як кількісні, так і якісні вимоги щодо кадрового складу, в той же час обсяги та структура облікових регістрів вибудовуються залежно від існуючих потреб системи управління.

Упровадження принципу документування передбачає також розробку системи умовних посилань від бухгалтерського звіту до первинного документа, що є основою для його складання. Під розробкою цієї системи треба розуміти встановлення порядку нумерування первинних документів під час їх складання та в процесі їх реєстрації в облікових регістрах.

Забезпечення принципу індивідуалізації досягається шляхом класифікації облікової інформації під час її документування за встановленими класифікаційними ознаками.

Принцип збереження в організації процесу документування означає встановлення та забезпечення термінів і умов зберігання облікової інформації в документах. Для впровадження зазначеного принципу доцільним є розробка відповідних процедур зберігання, закріплення конкретних осіб, відповідальних за збереження облікової інформації, порядку архівації носіїв (бухгалтерських документів, електронних носіїв облікової інформації), процедури та умов їх знищення з чітким визначенням кола відповідальних посадових осіб, їх повноважень і функцій у процесі збереження облікової інформації.

Організація процесу документування повинна дотримуватись принципу контрольованості облікової інформації. Необхідною умовою в цьому аспекті є впровадження системи внутрішнього контролю якості облікової інформації. Слід ураховувати, що встановлення обсягів та методів контролю визначається специфікою суб'єкта господарювання, кількісним складом співробітників, характером та обсягами облікової інформації, формою бухгалтерського обліку, що використовується підприємством, та обраною технікою обробки облікової інформації.

Принцип документування діяльності системи внутрішнього контролю має на увазі, що облікова інформація буде більш правильно оцінюватися керівництвом суб'єкта господарювання, загалом внутрішніми та зовнішніми користувачами, якщо організаційна структура системи внутрішнього контролю та її поточна діяльність документується в письмовому вигляді.

Автоматизація процесу документування облікової інформації дозволяє відмовитись від значної кількості паперових документів. То є суттєвою перевагою, і автор підтримує думку проф. І. Д. Фаріона [4, с. 70], що організація бухгалтерського обліку має бути такою, щоб забезпечити мінімальний шлях збирання та обробки інформації, мінімальну кількість операцій і документів, максимальну ефективність праці виконавців. Слід брати до уваги, що можливість відмови від паперових носіїв обумовлює виникнення проблеми нехтування робітниками підприємства паперовими документами загалом, що йде всупереч з принципом документального підтвердження облікової інформації та може сприяти маніпуляціям, перекрученню інформації та шахрайству, оскільки політика відмови від оформлення первинних документів на паперових носіях унеможливлює наочну доказовість факту господарського життя та відповідальності посадової особи, що брала участь у здійсненні господарської операції. Тому вважаємо, що будь-яка господарська операція повинна бути підтверджена первинним бухгалтерським документом, що складений (або відтворений) у паперовій формі.

Загалом застосування запропонованих напрямків організації процесу документування, що визначені з огляду на синергічний підхід, забезпечить належний рівень якості облікової інформації, ефективність інформатизації системи управління суб'єктів господарювання.

Література: 1. Хорнгрен Ч. Управленческий учет: Пер. с англ. / Ч. Хорнгрен, Дж. Фостер, Ш. Датар. – 10-е изд. – СПб.: Питер, 2005. – 1008 с. 2. Бетге Йорг. Балансоведение: Пер. с нем. / Науч. ред. В. Д. Новодворский. – М.: Изд. "Бухгалтерский учет", 2000. – 456 с. 3. Олійник В. М. Організація технології облікового процесу в агро формуваннях ринкового типу // Матеріали Міжнар. наук.-практ. конф. "Створення інтелектуальної системи обліку для економіки України", 21 – 22 листопада 2007 р. – Тернопіль: Економічна думка, 2007. – С. 59 – 61. 4. Фаріон І. Д. Зміст і передумови організації бухгалтерського обліку, аналізу та контролю // Матеріали Міжнар. наук.-практ. конф. "Створення інтелектуальної системи обліку для економіки України", 21 – 22 листопада 2007 р. – Тернопіль: Економічна думка, 2007. – С. 68 – 71.

Жукарєв В. Ю.

УДК 658.016.7

ЗАСТОСУВАННЯ МЕТОДУ МОНТЕ-КАРЛО ПРИ ПРИЙНЯТТІ УПРАВЛІНСЬКИХ ТРАНСФОРМАЦІЙНИХ РІШЕНЬ ЗА ДОПОМОГОЮ ПАКЕТА STATISTICA

Сьогодні відбувається велика кількість трансформаційних процесів на підприємствах України, які пов'язані як зі зміною власника, так і з іншими організаційно-економічними змінами, обумовленими впливом факторів як зовнішнього, так і внутрішнього середовищ. Трансформаційним процесам властива велика ступінь невизначеності, тому особі, що приймає рішення (ОПР), необхідно прогнозувати діяльність підприємства на певний період часу під впливом різних факторів. Прогнозування успішності прийняття управлінського трансформаційного рішення за допомогою врахування впливу факторів на об'єкт трансформації та скорочення невизначеності дозволяє застосування методу Монте-Карло.

Як зазначає І. М. Соболь [1], прогнозування є сполучною ланкою між теорією й практикою у всіх сферах життя суспільства та основою для формування державної політики.

Прогноз – це аргументоване висловлення про раніше не відоме й те, що не піддається поки що безпосередньому спостереженню, майбутній стан об'єкта і його опосередкованих зв'язків [2]. Це висловлення формується на основі специфічної наукової теорії, як висновок із сукупності конкретних подань про закономірності й тенденції розвитку об'єкта, про гіпотези й ідеї щодо майбутніх можливостей розвитку, а також про певні потреби та умови розвитку прогнозованого об'єкта.

Сьогодні різні методи й моделі прогнозування досліджені в роботах як вітчизняних, так і закордонних учених [1; 3]. У той же час питанням прогнозування, пов'язаним із трансформаційними перетвореннями на підприємстві, що відносяться до сфери корінних організаційних перетворень, усе ще приділяється недостатня увага. Тому однією з актуальних проблем, яка потребує вивчення, є можливість прогнозування діяльності підприємства для успішного прийняття управлінських трансформаційних рішень.

Метою статті є розгляд можливості використання імітаційного моделювання при прогнозуванні ймовірності успішного проведення зміни власника на підприємстві за допомогою пакета STATISTICA.

Одним із найпоширеніших методів прогнозного моделювання є імітаційне моделювання [3]. Це пов'язано з тим, що більшість реальних об'єктів (підприємств, організацій та ін.) внаслідок своєї складності не можуть бути реально описані за допомогою тільки аналітичних чи математичних моделей. Важливим фактором при виборі методу імітаційного моделювання є той факт, що імітаційна модель дозволяє використовувати всю розташовувану інформацію поза залежністю від її форми подання й ступеня формалізації.

Якщо вхідні параметри та (або) параметри моделі можуть мати випадкові значення, то говорять про моделювання у випадкових умовах, при цьому модель називається статистичною [3].

Для статистичного моделювання у випадкових умовах був розроблений метод статистичних випробувань (метод Монте-Карло). Ідея методу полягає в тому, щоб робити "розіграш" – моделювання випадкового явища за допомогою спеціально організованої процедури, що дає випадковий результат [1].

Виходячи із зазначеного, найбільш оптимально до вирішення поставленого трансформаційного завдання, а саме прогнозування ймовірності проведення зміни власника на підприємстві, підходить метод Монте-Карло.

У ході дослідження була висунута гіпотеза, що на проведення зміни власника підприємства впливає фінансовий стан підприємства, який характеризується наступними показниками: коефіцієнт поточної ліквідності, коефіцієнт автономії, питома вага основних засобів і продуктивність праці. Проаналізуємо вплив цих коефіцієнтів на проведення зміни власника на підприємстві.

При цьому коефіцієнт поточної ліквідності розраховується за формулою:

$$К_Л = О_А/П_З, \quad (1)$$

де $О_А$ – оборотні активи за поточний період;

$П_З$ – поточні зобов'язання за поточний період.

Коефіцієнт автономії розраховується за формулою:

$$К_А = В_К/(Д_З + П_З), \quad (2)$$

де $В_К$ – власний капітал за поточний період;

$Д_З$ – довгострокові зобов'язання за поточний період.

Питома вага основних засобів розраховується за формулою:

$$П_В = Н_А/П, \quad (3)$$

де $Н_А$ – необоротні активи за поточний період;
П – пасив підприємства за поточний період.

Продуктивність праці розраховується за формулою:

$$П_П = Н_П / Ч_П, \quad (4)$$

де $Н_П$ – нерозподілений прибуток (непокритий збиток) за поточний період;
$Ч_П$ – чисельність працівників за поточний період.

Для перевірки даної гіпотези були зібрані дані з 36-ти підприємств України. З обраних підприємств 25 перебувають у приватній власності, а 11 або повністю, або частково – у власності держави, при цьому на даних 11 підприємствах повинна відбутися зміна власника, а саме – приватизація. Для більш коректного відображення у вибірці беруть участь тільки підприємства харчової промисловості.

Для дослідження має сенс провести стандартизацію, яка дозволить при побудові моделі використовувати однакову шкалу виміру показників. Стандартизація здійснюється відповідно до формули, запропонованої В. Плютою в роботі [4]:

$$z_{ik} = \frac{p_{ik} - \overline{p_k}}{S_k}, \quad (5)$$

причому

$$\overline{p_k} = \frac{1}{t}\sum_{i=1}^{t} p_{ik}, \quad (6)$$

$$S_k = \left[\frac{1}{t}\sum_{i=1}^{t}\left(p_{ik} - \overline{p_k}\right)^2\right]^{\frac{1}{2}}, \quad (7)$$

де p_{ik} – значення показника діяльності підприємства k на і-му підприємстві;
$\overline{p_k}$ – середнє арифметичне значення показника k;
S_k – стандартне відхилення ознаки k;
z_{ik} – стандартизоване значення ознаки k для і-го підприємства;
k – показник діяльності підприємства, а саме фондоозброєність, рентабельність чи ефективність роботи персоналу;
i = 1, 2, …, t – кількість підприємств.

Процедура стандартизації ознак, відповідно до джерела [4], приводить не тільки до вирівнювання значень ознак, а й до елюмінування одиниць виміру.

Для проведення стандартизації автором використовувався табличний процесор Microsoft Excel 2003.

Для знаходження кореляційної залежності показників коефіцієнта поточної ліквідності, коефіцієнта автономії, питомої ваги основних засобів, продуктивності праці та ймовірності зміни власника за допомогою пакета STATISTICA була складена кореляційна матриця, подана на рис. 1.

Показнику перетворення привласнюється значення відповідного поточного стану підприємства:
1 – якщо підприємство перебуває в стадії зміни власника;
0 – підприємство вже змінило власника або не збирається проводити перетворень щодо зміни власника.

	1 КЛ	2 КА	3 ПВ	4 ПП	5 **Перетворення**
КЛ	1	0,95364	-0,15570	0,26053	-0,06297
КА	0,95364	1	0,05288	0,20502	0,08561
ПВ	-0,15570	0,05288	1	-0,25403	0,41859
ПП	0,26053	0,20502	-0,25403	1	-0,07946
Перетворення	-0,06297	0,08561	0,41859	-0,07946	1
Means	-0,00000	0,00000	0,00000	0,00000	0,30556
Std.Dev.	1,00000	1,00000	1,00000	1,00000	0,46718
No.Cases	36,00000				
Matrix	1,00000				

Рис. 1. **Матриця кореляційної залежності показників**

На підставі даної матриці (рис. 1), за допомогою пакета STATISTICA проводилось імітаційне моделювання з використанням методу Монте-Карло, в ході якого було задано, що показники коефіцієнта поточної ліквідності, коефіцієнта автономії, питомої ваги основних засобів і продуктивності праці впливають на перетворення.

Під час моделювання визначено сукупність випадкових величин для 100 значень за заданими критеріями.

Результат імітаційного моделювання наведений у графічному вигляді на рис. 2 – 5.

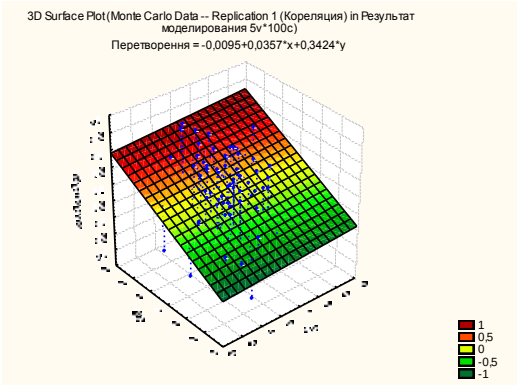


Рис. 2. **Вплив перетворення на коефіцієнт поточної ліквідності та коефіцієнт автономії засобів за результатами імітаційного моделювання, проведеного за допомогою методу Монте-Карло**

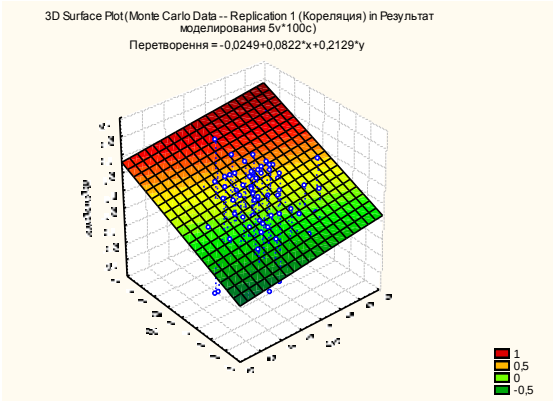


Рис. 3. **Вплив перетворення на коефіцієнт поточної ліквідності та питому вагу основних засобів за результатами імітаційного моделювання, проведеного за допомогою методу Монте-Карло**

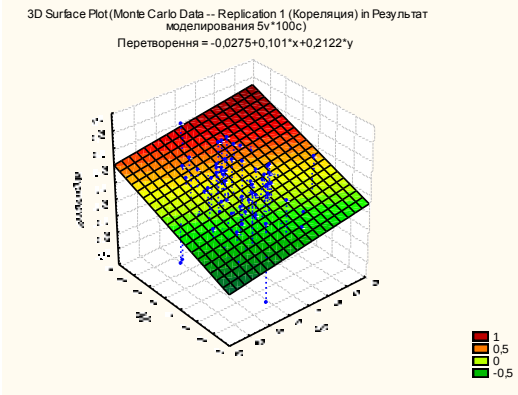


Рис. 4. **Вплив перетворення на коефіцієнт поточної ліквідності та продуктивність праці засобів за результатами імітаційного моделювання, проведеного за допомогою методу Монте-Карло**

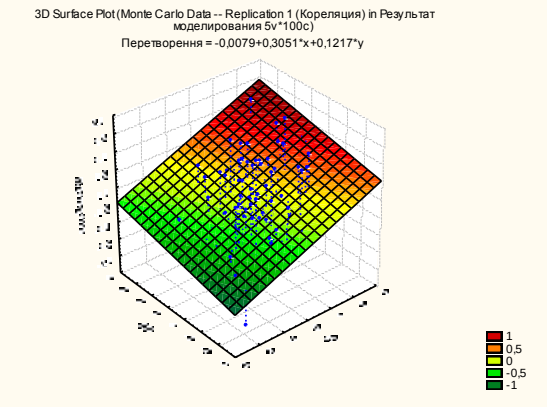


Рис. 5. **Вплив перетворення на коефіцієнт автономії та продуктивність праці засобів за результатами імітаційного моделювання, проведеного за допомогою методу Монте-Карло**

Як бачимо з рис. 2 – 5, перетворення позитивно впливають на всі розглянуті показники підприємства. Але зміна власника найменше впливає на коєфіцієнт ліквідності.

У ході дослідження за допомогою пакета STATISTICA була визначена лінійна залежність впливу на показник перетворення коефіцієнта поточної ліквідності, коефіцієнта автономії, питомої ваги основних засобів і продуктивності праці. На підставі цих даних складено оптимізаційну модель:

$$\begin{cases} П = -0{,}0095 + 0{,}0357 \times К_Л + 0{,}3424 \times К_А \\ П = -0{,}0079 + 0{,}3051 \times К_А + 0{,}1217 \times П_П \\ П = -0{,}0275 + 0{,}101 \times К_Л + 0{,}2122 \times П_П \\ П = -0{,}0249 + 0{,}0822 \times К_Л + 0{,}2129 \times П_В \end{cases}, \quad (8)$$

де П – коефіцієнт перетворення.

Після побудови оптимізаційної моделі (8) за допомогою функції прийняття рішення в табличному процесорі Excel можна визначити оптимальні значення показників коефіцієнта поточної ліквідності, коефіцієнта автономії, питомої ваги основних засобів і продуктивності праці підприємства для проведення зміни власника.

Застосування методу статистичних випробувань (методу Монте-Карло) дозволяє за допомогою використання наявних даних за схожими трансформаційними процесами дати підпри-

ємству відповідь на запитання, чи проводити відповідні корінні перетворення в цей момент часу або провести незначні зміни для корегування окремих показників, після чого приймати рішення щодо необхідності проведення трансформаційних перетворень. Використання пакета STATISTICA дозволяє більш зручніше та швидше апробовувати моделі, побудовані за допомогою методу Монте-Карло.

Література: 1. Соболь И. М. Метод Монте-Карло. – М.: Наука, 1968. – 64 с. 2. Добров Г. М. Прогнозирование науки и техники. – М.: Наука, 1969. – 208 с. 3. Глущенко В. В. Разработка управленческого решения. Прогнозирование – планирование. Теория проектирования экспериментов. – Железнодорожный, Моск. обл.: ООО НПЦ "Крылья", 2000. – 400 с. 4. Плюта В. Сравнительный многомерный анализ в экономических исследованиях: Методы таксономии и факторного анализа / Пер. с польск. В. В. Иванова. – М.: Статистика, 1980. – 152 с.

УДК 004.78:343

Хомич В. М.

Ходасевич А. А.

ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В ОБЛАСТИ ВЫСОКИХ ТЕХНОЛОГИЙ

В XX в. научно-технический прогресс (НТП) обеспечил кардинальную трансформацию систем информационного обмена и общения между людьми, существенно повлияв на многие сферы жизнедеятельности и образ жизни человека. Одним из важнейших средств коммуникации стали компьютерные сети (прежде всего, сеть Интернет). Новый способ взаимодействия проникает во все сферы жизнедеятельности человека и в ряде случаев кардинально меняет условия существования общества и конкретных людей. Обыденным стало широкое использование систем передачи информации в экономике, социальной сфере, культуре, науке, образовании, медицине и в иных областях. Оказывая воздействие на все сферы человеческой деятельности, ИТ в области связи и передачи информации особенно сильно влияет на экономическую жизнь. Поскольку хозяйственная деятельность с использованием ИТ имеет существенные особенности, ее стали обособлять при помощи специального термина − "электронная коммерция". Несмотря на серьезные технические, организационные, психологические и юридические препятствия для ее развития, электронная коммерция превращается в один из распространенных методов экономической активности. Однако скорость, с которой разрабатываются и внедряются в повседневную жизнь технические достижения в сфере информационного обмена, настолько высока, что право во многих случаях не успевает обеспечивать их практическое применение. Так, широкое распространение электронной коммерции порождает и другое явление − правонарушения, преступность в области высоких технологий. Правительствами многих стран делается попытка урегулирования виртуального пространства: разрабатываются проекты новых законов. Сегодня Интернет используется для террористических, экстремистских целей, а также других актуальных проблем, главным образом финансовых преступлений: фальшивое предложение товаров и услуг, услуги мошенников, связанные с платежными системами, онлайновские аукционы, Интернет-площадки для проведения тендеров.

К примеру, в Российской Федерации за 2006 год в сравнении с 2005 годом количество зарегистрированных преступлений возросло с 8 400 до 15 000, в сравнении с 1990 годом было выявлено всего лишь 10 − 12 преступлений, эти правонарушения носили больше хулиганский характер [1]. Сейчас две трети из всех преступлений в сфере высоких технологий имеют отношение к краже информации и несанкционированному доступу к этой информации, существенный сектор правонарушений связан с проведением онлайновских аукционов, размещением так называемых Интернет-площадок для проведения тендеров (торгов). В Уголовном кодексе Российской Федерации введена 28 глава, предусматривающая ответственность за преступления в сфере высоких технологий [2]. Существует также отдел при Министерстве внутренних дел Российской Федерации, региональный департамент по борьбе с компьютерными преступлениями, с незаконным распространением технических средств, мошенничеством в области электронных платежных систем. Число фальшивых сделок через Интернет-магазин растет, особенно когда платеж обрабатывается через систему Web Money. Новые методы шантажа − электронный шантаж, сотовый шантаж. К сожалению, существуют проблемы с законодательством в этой сфере. Сегодня не существует единых конкретных средств или правил по размещению информации в Интернете. Если веб-сайт носит, к примеру, террористический характер, то можно связаться с провайдером и просить о блокировании данного сайта, но что мешает создать новый веб-сайт и разместить ту же информацию. Хотелось бы исключить анонимность при подписании соглашения о телекоммуникационных услугах с

провайдером, необходимо, чтобы провайдер имел право в одностороннем порядке расторгнуть соглашении на основании постановления правоохранительных органов.

Что касается международного сотрудничества, то существует сеть организаций, имеющих свою единицу измерения передачи информации. Сотрудники специальных подразделений из одной страны могут в любое время суток связаться с той же единицей в другой стране и получить или предоставить данные, необходимые для проведения расследования. Эффективность данных подразделений доказана успешным раскрытием правонарушений. Глобальный характер, который носят компьютерные сети, а также то, что они затрагивают все сферы жизнедеятельности человека, не позволяет говорить о том, что перед правом стала задача регламентации ординарного технического новшества. Проблемы, связанные с правовым урегулированием ИТ, отнюдь не сводятся к трансформации действующего права и выработке совокупности новых правовых предписаний, отражающих специфику современных технологий обмена информацией. Социальные последствия некоторых новаций в осуществлении связи и передачи информации оказались столь широкими и всеобъемлющими, что перед обществом встали проблемы, которые не могут быть решены лишь на уровне права, а требуют широкого философского осмысления. Прежде всего, это вопрос о том, должны ли все аспекты коммуникаций в информационных сетях регулироваться государством или государства могут допустить в определенных пределах возможность автономного существования и саморегуляции в информационно-коммуникационном пространстве. В более широком плане нуждается в разрешении вопрос о том, распространяется ли государственный суверенитет на коммуникационные сети и обмен информацией в них, а также на создаваемое информационными сетями так называемое "киберпространство".

Прежде всего, связано с этим понятие "кибертерроризм", направленное на разжигание националистических, расовых предрассудков и нетерпимости. К сожалению, сегодня нет правовой базы, направленной на предотвращение таких явлений в сфере высоких технологий, кроме как заблокировать такой веб-сайт, но нет никаких правовых актов. Необходимо привести статистические данные. Так в Республике Беларусь за 2006 год совершено 272 преступления, связанных с "информационной безопасностью", 12 – с "несанкционированным доступом", 19 – с разработкой вирусных программ, которые были доведены до суда. По словам Игоря Черненко, начальника отдела преступлений в области высоких технологий МВД Республики Беларусь, в соответствии с действующим законодательством Республики Беларусь невозможно привлечь кого-либо к уголовной ответственности за операции в сфере высоких технологий, так как в Уголовном кодексе Республики Беларусь [3] ничего не говорится, к примеру, о распространении порнографии в сети Интернет, а привлечь можно только после того, как лицо в течение года привлекалось к гражданской ответственности [4]. За клевету в Интернете [5] можно привлечь к уголовной ответственности по ст.188 Уголовного кодекса Республики Беларусь. Также состояние информационной безопасности среди юридических и физических лиц сведена к нулю. Речь, конечно, не о сплетнях в чатах, а об экономической информации: взлом сайтов, наличие "черной бухгалтерии", использование доступа к коммерческим секретам фирмы в своих корыстных целях, использование контрафактного компьютерного обеспечения. Так, на Украине правоохранительными органами был задержан 17-летний житель Киева, который произвел взлом в платежной системе. При посредничестве российских и британских правоохранительных органов были задержаны три хакера. Они обвинялись в совершении вымогательства на сумму 4 млн долл. США от мировых Интернет-компаний (Can bet Sport Bookmaker Ltd, которая отказалась платить 10 000 долл. выкупа за информацию, вследствие чего она потеряла 200 000 долл. за каждый день простоя). Они собирали информацию о британских веб-казино и букмекерских конторах, об участниках проведения тендеров на Интернет-площадках с использованием программного обеспечения, а затем требовали выкуп данной информации от владельцев, угрожая "сорвать" их веб-серверы, если они не выполнят требования. Следователи ФБР, Интерпола и российских правоохранительных органов заявили, что преступная организация получила более 4 млн долл. США от британских компаний, группа действовала в 30 странах и совершила около 54 нападений. Совершенно очевидно, что попытки разрешения указанных вопросов каждым из государств обособленно не будут иметь успеха. Специфика новых коммуникационных технологий состоит, прежде всего, в том, что они по самой своей природе носят трансграничный характер. Это обстоятельство предопределяет роль и значение международного права в регламентации отношений в области связи и обмена информацией.

Необходимо отметить важность проведения международных конференций, к примеру, была проведена такого рода международная конференция в России, где были приглашены сотрудники правоохранительных органов из десятков стран, ученые, представители ООН, Европейского Совета и других органов. Было предложено три проекта: "Чистый Интернет", "Чистый код", "Чистое соединение". Так, к примеру, "Чистый код" предназначен для международного сотрудничества в борьбе с компьютерным мошенничеством при проведении электронной коммерции, что вызывает огромный ущерб для граждан и предприятий. Проект "Чистый Интернет" заключается в том, чтобы бороться с незаконным использованием сети Интернета для террористических целей, совместно выявлять экстремистские сайтов и противодействовать их деятельности [6].

При поддержке российского и белорусского правительств ежегодно проводится Международная научно-практическая конференция "Комплексная защита информации". В числе организаторов конференции – Парламентское Собрание Союза Беларуси и России, Постоянный Комитет Союзного государства, Совет Безопасности РФ, Государственная Дума РФ, Федеральное агентство по информационным технологиям Российской Федерации ("Росинформтехнология"), Государственный центр безопасности информации при Президенте Республики Беларусь, Федеральная

служба по техническому и экспортному контролю (ФСТЭК России), Всероссийский НИИ проблем вычислительной техники и информатизации (ВНИИПВТИ), Российско-белорусский журнал "Управление защитой информации".

Широкое распространение и многообразие проявлений электронной экономической деятельности привели к тому, что понятие "электронная коммерция" получает самые различные интерпретации. Следствием этого стало отсутствие четкого и исчерпывающего правового регулирования данного феномена. Как отдельными государствами, так и на международном уровне предпринимаются меры для установления единообразного регулирования.

Сложность исследования коммерческого взаимодействия в информационных сетях предопределяется широким кругом вопросов, которые затрагиваются электронной экономической деятельностью (проблемы электронного документооборота, юрисдикции и применимого права, обеспечения безопасности информационного обмена и пр.).

Предопределена практическая значимость, которая состоит в том, что основные положения, выводы и рекомендации, сформулированные в исследовании, могут быть использованы при формировании и совершенствовании международно-правового регулирования коммуникационных технологий, электронного документооборота и электронной коммерции, а также при совершенствовании национального законодательства. В исследовании авторами приведены конкретные примеры недееспособности законодательства по формированию механизма правового регулирования новых технологий коммерческой деятельности на международном и национальном уровнях. Практическая значимость исследования заключается в том, что содержащиеся в работе положения и выводы могут быть использованы соответствующими международными органами и организациями, представителями государств, в практической деятельности по созданию международно-правовых норм в области электронного документооборота и электронной коммерции. Рекомендации программистов могли бы решить многие вопросы для совершенствования электронной коммерции.

Литература: 1. Уголовный кодекс Российской Федерации: Принят Государственной Думой 24.05.1996, одобрен Советом Федерации 5.06.1996. Гл. 28. Ст. 272 – 274. 2. Уголовный Кодекс Республики Беларусь: Принят Палатой представителей 2.06.1999, одобрен Советом Республики 24.06.1999, от 9.07.1999 №275-З / НРПА Республики Беларусь. – 2006. – №122, 2/1295. – Гл. 22, ст. 188, гл. 31, ст. 349 – 355. 3. Computer Crime Research Center / www. crime-research. org /analytics/cyber_crimes01081 January 03.2008 / Cyber-crimes Analytical Data Compiled / Vladimir Golubev. 4. Постановление Совета Министров Республики Беларусь от 10.02.2007 №175 "Об утверждении Положения о порядке работы компьютерных клубов и Интернет-кафе" / НРПА Республики Беларусь 5/24720, от 14.02.2007. 5. Черненко Игорь. Регистрация по паспорту в Интернет-кафе не прошла, 17.02.2007 // www. bybanner. com / article / 4167.html ". 6. Черненко Игорь. Отвечает на вопросы об информационной безопасности предприятий. 11.05.2007 // www. security. tut. by

УДК 681.3

Лукацкий А. В.

СВЯЗЬ БЕЗОПАСНОСТИ КОМПАНИИ С ЕЕ БИЗНЕСОМ

Безопасность способствует или мешает? Как обычно говорят окружающие: "Отдел информационной безопасности − люди? Что они от нас хотят? Мы занимаемся делом, а тут они… Только тратят заработанные нами деньги и занимаются непонятно чем. Еще придумывают новые и незапоминающиеся пароли, читают мою почту, запрещают мне работать в Интернете и делают мою жизнь только сложнее". Так уж сложилось на протяжении последних лет. Но мы вынуждены жить… и мириться с этим. Но… давайте сломаем эти стереотипы и покажем всем, что такое информационная безопасность (ИБ) на самом деле.

Нередко на Западе безопасность называют "Business Prevention", то есть блокирующей, а не способствующей бизнесу, и такое отношение не случайно − оно формировалось годами. Вышедшая из недр государственной и военной машины, информационная безопасность изначально была ориентирована совсем на другое − "закрыть", "запретить", "не дать", "блокировать" и т. п. И перейдя на службу бизнеса, она во многом осталась такой же. Однако бизнес требует от безопасности совершенно иного.

Будучи одним из внутренних процессов компании, она, как и все другие, должна быть направлена на достижение поставленных бизнесом целей. Если же мы не можем сказать, что мы даем бизнесу, то зачем мы вообще сидим на своем рабочем месте. Может стоит заняться чем-то более понятным и адекватным? Даже уборщица делает для бизнеса больше, чем типичный безопасник. Она чистит офис, делая работу в нем приятной, что благотворно влияет и на климат в

коллективе, и на бизнес-показатели. А безопасник? Достаточно провести мини-опрос среди сотрудников или хотя бы руководителей бизнес-подразделений и все сразу встанет на свои места – службу ИБ все считают только мешающей бизнес-процессам. И она будет помехой, пока мы не покажем ее преимущества тем, кто считает ее препятствием. Как это сделать? [1]

Целью статьи является наглядный показ связи безопасности компании с ее бизнесом для руководителей компаний.

Существует классическая дорожная карта, насчитывающая всего 5 шагов, которые помогут вывести безопасность на качественно новый уровень. Сразу надо отметить, что эти шаги применимы практически к любой деятельности, которую надо привести в соответствие с бизнес-стратегией предприятия. Итак, эти шаги следующие:

1. Оценка текущей ситуации. На этом этапе составляем картину состояния информационной безопасности в компании. Иными словами, мы отвечаем на вопрос: "Как есть сейчас?" или "Где мы находимся?"

2. Анализ потребностей бизнеса. Второй шаг помогает определить, ради чего существует компания, какие стратегические и тактические задачи стоят перед различными подразделениями, какова бизнес-среда и т. д.

3. Планирование будущей архитектуры ИБ. Результатом этого шага является ответ на вопрос: "Как должно быть?"; при этом мы учитываем имеющиеся потребности бизнеса.

4. Анализ разрыва. На этом этапе оцениваем различия между текущим и планируемым состоянием.

5. Способы сокращения разрыва. Заключительный этап позволяет определить конкретные мероприятия по достижению будущей архитектуры ИБ, их стоимость и временные затраты.

Разумеется, для того, чтобы движение по этой дорожной карте было не только результативным, но и оптимальным, должны учитывать ключевые факторы успеха, которых в нашем случае тоже пять:

отказ от птичьего и использование общего с бизнесом языка;

эффективный процесс взаимодействия со всеми бизнес-подразделениями;

внедрение системы внутреннего маркетинга ИБ;

выход на руководство;

измерение эффективности процесса ИБ.

Вспомним басню Крылова про лебедя, рака и щуку. Информационная безопасность сегодня находится именно в такой ситуации – цели ИБ не совпадают с целями бизнеса. Безопасность думает о криптографии, межсетевых экранах, антивирусах, восстановлении после катастроф, защите от хостов и т. д. Думает ли об этом бизнес? Вряд ли. У него совершенно иные заботы. Управление рисками, обеспечение непрерывности бизнеса, соответствие регулятивным требованиям (compliance), внутренний контроль, корпоративное поведение, рост лояльности клиентов, слияния и поглощения, географическая экспансия и многое другое. Видим, что совпадений нет. Это как общение англичанина с китайцем – каждый общается на своем языке и не понимает другого. Но есть одно, что объединяет безопасника с сотрудником бизнес-подразделений. Речь идет о бизнес-целях, которые у них общие.

Не всегда безопасность может быть связана напрямую с целью всей компании. Но это и не всегда требуется. Мы можем увязать ИБ с целями отдельного подразделения, проекта, инициативы или человека-"спонсора". При этом вопреки распространенному мнению, что цель коммерческого предприятия всегда завязана на финансы, надо отметить, что это не всегда так. Помимо роста доходов, снижения издержек, роста рентабельности и других монетарных целей, бизнес может ставить перед собой и другие задачи – рост лояльности и снижение текучести клиентов, географическая экспансия, ускорение сроков вывода продуктов на рынок, выполнение требований стандарта (например, пресловутого SOX) и т. п. Главное, чтобы мы смогли связать ИБ с этими целями. Можно ли это сделать? Да, можно. Разумеется, что только в том случае, если мы понимаем бизнес, которым занимается компания. В качестве примера и в условиях ограниченного объема для статьи возьмем только одну поставленную бизнесом задачу – рост продуктивности сотрудников [1].

Эта задача может быть решена по-разному; один из вариантов – внедрение концепции Network Virtual Organization, которая гласит, что "офис там, где сотрудник", а не "сотрудник там, где офис". Эта концепция подразумевает, что сотрудник находится все время "в поле" как можно ближе к своим проектам, клиентам, партнерам и т. п. Но чтобы быть эффективным, он должен быть не только все время на связи, но и иметь доступ к корпоративным информационным ресурсам. При такой постановке задачи каждый сотрудник оснащается лэптопом или КПК с различными интерфейсами подключения к сети (CDMA, GPRS, UMTS, Wi-Fi и т. п.), встроенным клиентом IP-телефонии, почтовым клиентом и другими полезными приложениями. В итоге сотрудник становится мобильным, но для всех он как будто по-прежнему находится на своем рабочем месте. По разным оценкам рост продуктивности сотрудника при использовании этой концепции может составлять от 10 до 40 процентов. А это, в свою очередь, говорит об экономической целесообразности внедрения таких решений. Помимо финансовой стороны вопроса, существует еще и психологические моменты. Учитывая темп жизни современного человека, он всегда стоит перед дилеммой – работа или семья. И он вынужден разрываться между домом и офисом. А это, в свою очередь,

стресс, что влияет на все стороны жизни человека, в том числе и работу. Концепция NVO является компромиссом, так как она дает возможность подключаться к корпоративной сети в любое удобное время и в любом удобном месте. Но мобильность несет с собой и угрозу, так как сотрудник уже не находится под защитой корпоративных систем защиты. В этом случае мы должны оснастить персональными средствами безопасности лэптопы сотрудников, а также модернизировать периметр сети для поддержки концепции NVO. И такая связь с безопасностью может быть прослежена во многих бизнес-задачах.

Процесс взаимодействия. Безопасность – это не задача не только одноименной службы, но и всех сотрудников предприятия. И для того чтобы они поняли это, требуется активное взаимодействие между службой ИБ и остальными подразделениями. Внедрение правильного подхода к ИБ – это всегда движение в обе стороны. Поэтому пора уходить от запретительной практики, так распространенной в нашей сфере. Любой запрет вызывает отрицательную реакцию, которая негативно сказывается на отношении к безопасности в целом. Достаточно вспомнить старую поговорку: "Будьте добрее и люди потянутся к вам". В безопасности все то же самое.

Система внутреннего маркетинга. Когда все хорошо, то часто можно слышать такие вопросы со стороны руководства или других подразделений: "Что вы сделали для меня в последнее время?" или "У нас давно не было атак. Зачем вы нам нужны?" Отсутствие видимых проблем – это тоже проблема! Наградой за эффективную и высококачественную, но незаметную работу будет отрицательная оценка со стороны руководства и бизнес-подразделений. Информационная безопасность – одна из важных задач любого предприятия. И при этом одна из малопонятных, "нерыночных" и нерекламируемых [2].

Наличие коммуникативного разрыва между службой ИБ и всем остальным миром привело к большому числу стереотипов в отношении безопасности, часть из которых мы уже упомянули ранее:

"они (то есть безопасники) являются помехой на пути к успеху";

"говорят на птичьем языке";

"они живут в изолированном мире";

"они сосредоточены на деталях и не могут окинуть бизнес общим взглядом";

"у них слишком развито чувство превосходства";

"они не заинтересованы в масштабных проектах".

Аналогичные стереотипы существуют и со стороны специалистов по ИБ в сторону всего остального мира:

"мы непонятые гении";

"мы люди второго сорта";

"мы жертвы обстоятельств";

"мы перегружены работой, нас не ценят, нам недоплачивают";

"нас нельзя винить в сбое "железа" и софта или потому что сеть "медленно работает".

Причина такого числа стереотипов в том, что большинство людей измеряет ИБ "своим аршином" и "с высоты своей колокольни". Но безопасность очень сильно отличается от того, к чему привык бизнес:

она сосредоточена на деталях;

скорость изменения технологий не всегда оставляет времени, чтобы остановиться и посмотреть на картину в целом;

ИБ находится в стадии становления;

многие стандартные практики не получили должного развития.

Именно поэтому необходимо ломать сложившиеся стереотипы – без этого проблемы и недоверие с обоих сторон будут только накапливаться. Чтобы сделать это, надо внедрять в компании коммуникативную практику в отношении ИБ. Иными словами, мы должны заниматься маркетингом и рекламой безопасности внутри компании, которые нужны не только производителям или поставщикам каких-либо товаров и услуг. К слову сказать, хороший маркетинг и коммуникации могут компенсировать отсутствие достаточной синхронизации ИБ с бизнесом (но злоупотреблять им не надо). Что такое внутренний маркетинг ИБ? Это искусство добиваться такого восприятия ИБ клиентом, при котором у него формируются приемлемые ожидания к деятельности поставщика услуг ИБ и отношения клиента и ИБ были взаимовыгодными. Клиент в данном случае – это собственные сотрудники.

Выход на руководство. Сами по себе проекты по информационной безопасности не защищаются и деньги на них не выдаются независимо от используемых метрик, привязки к бизнесу, коммуникативной практики и т. д. По-прежнему важен человеческий фактор – отсутствие умения "взаимодействовать" на уровне топ-менеджмента сводит "на нет" все предыдущие усилия и работу. Слово "взаимодействовать" не случайно вынесено в кавычки – за ним скрывается очень много оттенков и нюансов. Взаимодействие включает в себя три составляющие:

сила и влияние;

репутация;

знание психологии.

Сила и влияние – это всегда комбинация множества факторов, про каждый из которых можно написать целую статью:

знаний и информации;

привилегий;
доступных ресурсов;
уровня иерархии;
харизмы;
эмоций.

Коснемся только одного – уровня иерархии, как наиболее острого и дискуссионного. Сегодня все специалисты сходятся во мнении, что руководитель службы ИБ (Chief Information Security Officer, CISO) не может и не должен находиться в подчинении у CIO. Нельзя быть зависимым от CIO и оставаться эффективным. И не из-за желания стать выше, а из-за природы безопасности как функции контроля, которая должна быть независимой от контролируемых. Не случайно службы внутреннего контроля (внутреннего аудита) являются независимыми и контролируются непосредственно советом директоров. Информационная безопасность должна быть также независимой.

Другая причина, почему CISO должен быть выведен из под CIO – широкий спектр не ИТ-задач:

безопасность информации, представленной на бумаге или устно;
взаимодействие с HR;
взаимодействие с юристами;
взаимодействие с правоохранительными органами.

Такой спектр задач выходит за рамки деятельности CIO и, ставя приоритеты в своей работе, он будет решать их в самую последнюю очередь.

Но если не под CIO, то где? В настоящий момент наиболее правильным считается нахождение CISO на том же уровне иерархии, что и другой топ-менеджмент. Это обусловлено рядом причин. Во-первых, понижение в уровне приводит к невозможности эффективного решения многих задач – управление рисками, юридические вопросы и обеспечение непрерывности бизнеса и т. д. А во-вторых, из 80% внутренних атак только малая часть наносит большой ущерб и часто они исходят от руководства высокого уровня. Иными словами, борьба с инсайдерами должна вестись и на самом верхнем уровне компании, а это требует, чтобы CISO находился на том же уровне, что и топ-менеджмент.

Что касается психологии, то достаточно вспомнить слова Дейла Карнеги, сказанные им еще пару десятков лет назад: "*Единственный способ влиять на кого-либо – выяснить, что нужно этому человеку, и показать, как он этого может добиться*". Они имеют отношения, в том числе и к безопасности.

Измерение эффективности. Очень часто мы занимаемся безопасностью, не задумываясь, что и зачем мы делаем. Мы устанавливаем межсетевые экраны, обновляем антивирусы, проводим обучение сотрудников, повышаем осведомленность персонала, заказываем аудит, сертифицируемся на соответствие ISO 27001 и т. д. Но хорошо ли мы выполняем эти задачи? Как нам не только внешней (по отношению к нам) аудитории, но и самим себе продемонстрировать результативность своей работы? Нам не обойтись без измерения информационной безопасности с различных точек зрения. Однако измерение или демонстрация результатов своей работы – это не единственная причина задуматься об оценке процесса ИБ. Среди других целей можно назвать:

следование бизнес-ориентированному толкованию термина "информационная безопасность";
выполнение требований стандартов;
обоснование инвестиций.

Как говорится "безопасность стоит дорого, но она того стоит". Однако, чтобы доказать выделение немалых инвестиций, мы должны идти по пути борьбы с другими подразделениями, проектами и инициативами, которые тоже остро нуждаются в деньгах для своего существования. Выигрывает не тот, кто сильнее, а тот, кто более приспособлен. Этот закон эволюции применим и к финансированию. В условиях борьбы за презренный металл побеждает тот, кто сможет лучше обосновать запрашиваемые ресурсы и доказать, что они не утекут, как вода из крана, а принесут определенную отдачу. Как мы посмотрели ранее, такая отдача может выражаться не только в деньгах, но и в достижении бизнес-целей инвестора, в качестве которого может выступать компания в целом, бизнес-подразделение или владелец проекта/инициативы. И мы не можем уйти от измерений, которые и послужат необходимым доказательством. Причем измерений как с точки зрения запрашиваемых денег, так и с точки зрения оценки отдачи [2].

Если вспомнить про описанную выше дорожную карту, то любой из пяти этапов подразумевает те или иные измерения безопасности, ее эффективности, оптимальности и т. д. Но можно ли ее измерить? Бытует распространенное мнение, что это невозможно. Но вопреки ему необходимо отметить, что это совершенно не так. Доказать это можно с помощью обычной логической цепочки, проиллюстрированной на рисунке. Безопасность – это процесс, который мы внедряем для того, чтобы наступило улучшение в данной области. Если что-то лучше, то есть признаки этого улучшения. Конечно, внедрение процесса обеспечения информационной безопасности может и негативно сказаться на деятельности предприятия, но в любом случае у нас будут присутствовать признаки ухудшения. Отсутствие признаков говорит скорее о неумении их идентифицировать, чем о том, что их нет на самом деле. Присутствие признаков говорит о том, что их можно наблюдать, а наблюдаемое улучшение (или ухудшение) – посчитать и измерить. А уж коли мы можем измерить изменение состояния того или иного процесса, то мы можем и оценить его. А отсюда всего один шаг до демонстрации улучшений нужным людям, о которых мы говорили выше.

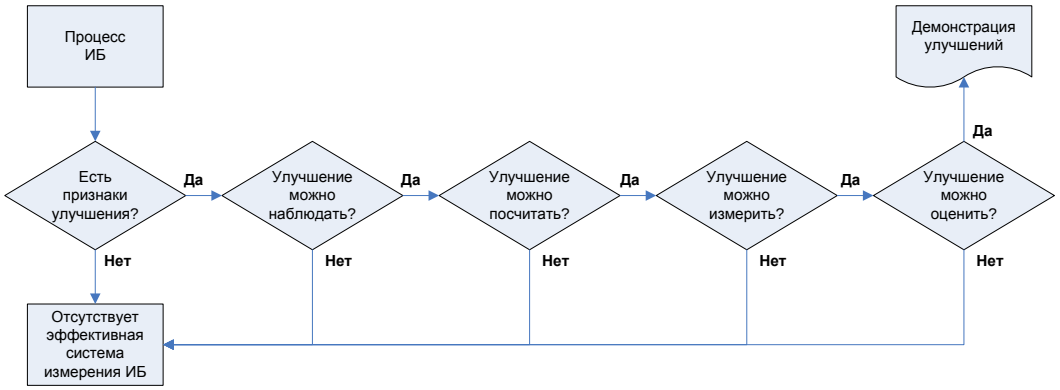


Рис. **Алгоритм развенчания мифа о невозможности измерения ИБ**

Методов измерения безопасности существует множество (вплоть до применения системы сбалансированных показателей или системы ключевых показателей деятельности) и мы их не будем рассматривать в данной статье по причине нехватки места.

Сделаем вывод, что пришла пора менять отношение к безопасности, как к чисто технологической задаче. Это совершенно не так. Она не только может осуществляться в контексте развития бизнеса, но и положительно влиять на многие бизнес-показатели развития предприятия. Надо только уметь отслеживать это влияние.

Литература: 1. http://www. ischool. berkeley. edu/~rachna/security_usability. html – набор ссылок на различные публикации об удобстве и безопасности. 2. Security and Usability. Lorrie Faith Cranor, Simson Garfinkel // TEER. – 1986. – 150 p.

УДК 519:37

Огурцов В. В.

Пономарьова К. В.

ВИКОРИСТАННЯ ВІРТУАЛІЗАЦІЇ В ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ У ВНЗ

У сучасних умовах стрімкого розвитку інформаційних технологій і як наслідок відчутного збільшення кількості різних програмних продуктів, комплексів та систем дуже складно встигати освоювати й адаптувати їх до освітньої діяльності. Але крім цієї проблеми, багате розмаїття програмного забезпечення (ПЗ) породжує проблему ефективного управління (адміністрування, встановлення, інвентаризації) цим ПЗ, яке використовується в навчальному процесі. Для забезпечення якості освіти викладачі повинні мати можливість застосовувати все потрібне ПЗ у навчальному процесі. Але, крім проблеми ефективного управління та ліцензування ПЗ, постає проблема несумісності різних програмних продуктів, конфліктів, які вони можуть викликати в операційній системі.

Вирішувати ці проблеми потрібно в межах комплексної оптимізації IT-інфраструктури вищого навчального закладу. Проблемою оптимізації IT-інфраструктури організацій активно займаються такі гіганти IT-індустрії, як Microsoft [1], Sun Microsystems [2], IBM [3] та ін. Вагому частину в стратегіях оптимізації IT-інфраструктури організацій, які пропонують та розвивають ці компанії, займає віртуалізація. При цьому віртуалізація розвивається в різних напрямках: віртуалізація операційних систем, віртуалізація застосувань, апаратна віртуалізація, віртуалізація сховищ даних, віртуалізація представлень, віртуалізація мережі.

На перший погляд може здаватися, що всі переваги віртуалізації нівелюються значним підвищенням апаратних вимог. Але це не так або не так у разі коректного застосування віртуалізації. Тому розглянемо суть різних видів віртуалізації, їхні переваги та недоліки.

Віртуалізація в IT-середовищі – це ізоляція одних комп'ютерних ресурсів від інших. За рахунок взаємного відділення різних рівнів логічної структури забезпечуються підвищена гнучкість і

спрощене управління змінами – більше не буде потрібно настроювати кожен елемент окремо для спільного використання з іншими [4].

Загальне порівняння традиційних наборів обладнання/ПЗ та відповідних віртуальних наведено в табл. 1.

Таблиця 1

Порівняння віртуальних і традиційних ІТ

Традиційний набір обладнання/ПЗ	Ізоляція компонентів за допомогою віртуалізації
Застосування встановлених на певному обладнанні або ОС	**Віртуальні застосування** Будь-яке застосування на будь-якому комп'ютері, доступне за вимогою
Інтерфейс, прив'язаний до процесу	**Віртуальне представлення** Рівень представлення відокремлений від процесу
Операційна система, призначена для конкретного обладнання	**Віртуальна машина** ОС може бути призначена будь-якому ПК або серверу
Системи зберігання, прив'язані до певного місця	**Віртуальне сховище** Зберігання та резервне копіювання по мережі
Мережа, прив'язана до певного місця	**Віртуальна мережа** Локалізація розосереджених ресурсів

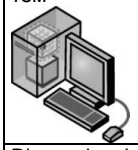
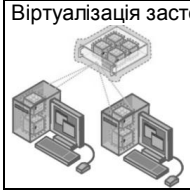
Щоб краще зрозуміти віртуалізацію, варто розглянути машинну віртуалізацію. В умовах машинної віртуалізації операційна система й застосування поєднуються та формують віртуальну машину, що розміщується потім на фізичному сервері під керуванням головної операційної системи, або гіпервізора (тонкого рівня ПЗ, що надає базові засоби для взаємодії з устаткуванням). Найважливіший елемент концепції полягає в тому, що віртуальна машина (ОС + застосування) працює незалежно від операційної системи, встановленої на фізичному сервері. Це дозволяє використовувати кілька віртуальних машин на одному фізичному сервері, одержуючи в результаті ту ж ізоляцію й безпеку, як і при застосуванні з цією метою виділеного устаткування.

Переваги машинної віртуалізації помітні, особливо якщо взяти до уваги, що більшість робочих навантажень використовують лише малу частину загальної потужності обладнання. При узгодженні навантажень відносно процесорної потужності й споживання пам'яті ІТ-організація може скоротити кількість фізичних серверів, які необхідні для підтримки бізнесу. Типовий рівень завантаження сервера становить від 5%, а 85% загальної потужності сервера не застосовуються. Підвищення рівня використання навіть до 60% означає чотириразове зменшення займаної площі, обсягу обладнання та енергоспоживання для живлення й охолодження цих серверних ферм. Цей процес називається об'єднанням серверів.

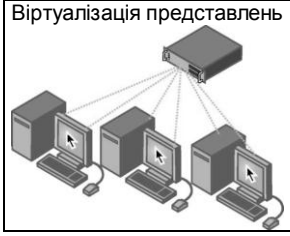
Концепція віртуалізації включає різні види віртуалізації, основні можливі варіанти використання яких наведено в табл. 2.

Таблиця 2

Основні варіанти застосування віртуалізації

Різновид віртуалізації	Приклад застосування
1	2
Віртуалізація сервера 	Забезпечує створення середовища окремої ОС, що логічно ізольована від головного сервера. Це дає підвищену ефективність використання ресурсів (обладнання, комунальні послуги, простір), а також ізоляцію й безпеку
Віртуалізація настільних систем 	Забезпечує створення середовища окремої ОС на настільному ПК, що дозволяє використовувати на комп'ютері несумісні застарілі або спеціалізовані застосування в сучасній версії ОС
Віртуалізація застосувань 	Відокремлює рівень конфігурації додатків від ОС у середовищі настільних ПК, що дозволяє знизити конфлікти додатків, здійснювати централізоване керування оновленнями й виправленнями, а також прискорити розгортання нових додатків і оновлених версій

Закінчення табл. 2

1	2
Віртуалізація представлень 	Забезпечує ізоляцію процесора від графічної підсистеми та засобів введення-виводу, що дозволяє запускати додаток в одному місці, а працювати з ним з іншого місця. Це може виявитися корисним у багатьох випадках, у тому числі коли дуже важливо забезпечити конфіденційність і захист даних

Інфраструктура, в якій добре реалізована віртуалізація, забезпечить зниження витрат, збільшення рівнів обслуговування й підвищення гнучкості. Зокрема, це досягається завдяки наступним особливостям.

Консолідація серверів. За рахунок консолідації навантажень на одній апаратній платформі можна підтримувати схему "одне застосування – один сервер", у той же час запобігаючи розростанню числа серверів. Це дозволить цілком забезпечити потреби бізнесу при меншій кількості обладнання, знизити витрати на обладнання, зменшити енергоспоживання на роботу й охолодження серверів, а також скоротити фізичну площу, необхідну для розміщення ферми серверів.

Максимізація корисного часу. За рахунок розподілу навантажень виключається вплив одного застосування на функціонування іншого та збої системи. У результаті навіть нестійке застаріле застосування зможе успішно працювати в безпечному, ізольованому середовищі.

Надійне аварійне відновлення. Стратегія віртуалізації дозволяє підтримувати план миттєвого аварійного відновлення, що забезпечить безперервність бізнесу у випадку ушкоджень. Маючи в наявності надійні засоби, можна впевнено виконувати автоматичне резервне копіювання, реплікацію й швидке переміщення серверів, настільних ОС і застосувань.

Скорочення регресивного тестування додатків на сумісність. За рахунок віртуалізації застосувань і надання їх на настільні ПК за запитом практично виключаються конфлікти застосувань між собою. Це значно скорочує регресивне тестування перед розгортанням і усуває більшість проблем із сумісністю.

Підтримка застарілих і спеціалізованих додатків. Служби терміналів або віртуалізація настільних систем дозволять новим ОС підтримувати застосування, написані для застарілих операційних платформ без виправлення їхніх програмних кодів.

Ефективне обслуговування серверів. Гнучкість розподілу навантажень між фізичними серверами з мінімальним збитком для їхньої роботи дозволяє планувати технічне обслуговування серверів без перерв в обслуговуванні бізнесу.

Оптимізоване введення в експлуатацію. Введення в експлуатацію робочих ресурсів можна прискорити та відокремити від процесу придбання обладнання. Якщо для якого-небудь певного бізнес-процесу потрібні додаткові можливості (наприклад, веб-механізм), їх можна миттєво й дуже просто отримати. У розширеному віртуалізованому середовищі робочі навантаження можуть самостійно визначати вимоги до ресурсів, забезпечуючи їхній динамічний розподіл.

Зниження складності. При управлінні віртуальною інфраструктурою за допомогою таких же засобів, які використовуються для фізичних активів, можна спростити складність і оптимізувати зміни, що вносяться у всю інфраструктуру.

Розглянемо більш детально варіант застосування віртуалізації в навчальному процесі у ВНЗ. На думку авторів, насамперед, значне спрощення управління IT-інфраструктурою навчального процесу забезпечить повсюдне (на кожній робочій станції, які використовуються в навчальному процесі) використання віртуальних машин. Найбільше спрощення та в той же час гнучкість забезпечить наступна схема управління IT-інфраструктурою навчального процесу:

1. На кожній робочій станції в несистемному розділі в стандартному каталозі розміщуються образи віртуальних дисків зі встановленими операційними системами, які використовуються в навчальному процесі.

2. Ці операційні системи мають базову конфігурацію (без установлення додаткового ПЗ, що специфічне для якої-небудь дисципліни).

3. Повні права доступу до базових файлів образів повинні мати тільки адміністратори.

4. Викладачі та студенти повинні мати тільки права на копіювання та виконання цих файлів.

5. На сервері у спільному каталозі викладачі за деякий час (залежно від кількості робочих станцій, які використовуються для викладання відповідної дисципліни), згідно із загальною політикою обчислювального центру, який обслуговує навчальні комп'ютерні класи, розміщують або оновлюють диференційні файли-образи жорстких дисків (differencing virtual hard drive) базової конфігурації. В цих файлах образів ОС зберігаються лише зміни щодо базової віртуальної ОС, які відбуваються під час встановлення та конфігурування відповідним викладачем потрібного ПЗ для дисциплін(и), що він викладає. На рисунку наведено приклад створення диференційного файла-образу жорсткого диска у MS Virtual PC 2007.

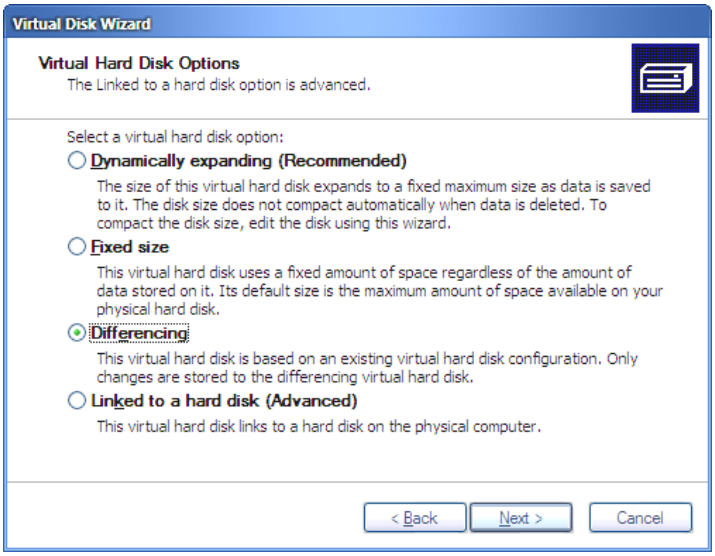


Рис. **Приклад створення диференційного файла-образу жорсткого диска у MS Virtual PC 2007**

6. Адміністратор здійснює копіювання відповідних диференційних файлів-образів у каталоги на робочі станції, які відведено для відповідної дисципліни. При цьому доступ на читання до цих каталогів (на сервері з локальної мережі та на робочих станціях) також мають студенти.

7. Для виконання лабораторних робіт студент повинен створити у відповідному каталозі (для роботи в цьому каталозі він має необхідні права) віртуальну машину з диференційним віртуальним жорстким диском щодо віртуального диску відповідної дисципліни.

8. Кожна хостова ОС повинна мати мінімальний типовий набір та конфігурацію встановленого програмного забезпечення, наприклад Microsoft Office.

Ця схема дозволить з мінімальними витратами використовувати в навчальному процесі різні ОС, різне ПЗ та зокрема:

адміністратору (обчислювальному центру, який обслуговує навчальні комп'ютерні класи):

спростити процес управління (встановлення, адміністрування та видалення) ПЗ навчальних робочих станцій (адміністратору в більшості доведеться слідкувати за використанням дискового простору або гнучко настроїти політики квотування дискового простору);

значно посилити надійність і безпеку;

викладачеві:

самостійно встановлювати та конфігурувати програмне середовище, як це найбільш потрібно для виконання лабораторних робіт за відповідної дисципліни;

оперативно реагувати в межах навчального процесу на зміни в IT-сфер;

студентам:

мати рівні умови навчання в комп'ютерних класах;

мати можливість виконувати лабораторні завдання під час самостійної роботи (наприклад, вдома);

відмінити дії і тільки ті дії, які вони зробили під час виконання лабораторної роботи, шляхом створення нового диференційного віртуального жорсткого диска щодо віртуального диска відповідної дисципліни.

Як недолік можна зазначити зростання апаратних вимог до робочих станцій і серверів. Але згідно з тенденцією помітного зростання потужностей комп'ютерів широкого використання й зниження їхньої вартості та відповідно до ціни цей недолік стає все менш значущим.

Також проблемою стає управління ліцензіями на віртуальні ОС та віртуальне ПЗ. Але ця проблема може бути вирішена завдяки укладанню договорів з розробниками ОС та ПЗ, наприклад, як у Microsoft існує форма взаємодії, що має назву MSDNAA (MSDN Academic Alliance), яка дає право використовувати в навчальному процесі ВНЗ більшість з продуктів компанії, зокрема операційні системи, безкоштовно. Така тенденція посилення співпраці компаній розробників різного ПЗ прослідкується останнім часом. Звісно, це результат плідної співпраці як активних співробітників ВНЗ, так і компаній-розробників ПЗ, що не менш зацікавлені в цій співпраці.

У підсумку можна відмітити важливість комплексної оптимізації IT-інфраструктури організацій і значну роль у ній концепції віртуалізації та, зокрема, використання цієї концепції у ВНЗ, що накладає свої особливості.

Література: 1. ИТ-инфраструктура // http://www. microsoft. com/rus/business/infrastructure/default. mspx 2. Эффективность ИТ-инфраструктуры: виртуализация на всех уровнях ИТ // http://www. pcweek. ru/white-papers/download. php?ID=104891. 3. Оптимизация ИТ-инфраструктуры // http://www. ibm. com/ru/events /presentations/bf2007/ 4. Создание всесторонней комплексной стратегии виртуализации // https://msdb. ru/downloads/virtualization/whitepaper-virtualization-coreio-fy08.pdf

УДК 681.325

Гринев Д. В.

Паржин Ю. В.

МЕТОД РАСПОЗНАВАНИЯ ПЕЧАТНОГО И РУКОПИСНОГО ТЕКСТА ПО СТРУКТУРНЫМ ТОЧКАМ

Стандартный подход к проблеме распознавания образов заключается в сведении задачи распознавания к задаче классификации некоторого набора признаков. В системе существует некоторое количество эталонов, которые обладают определенным набором признаков. Символ, который нужно распознать, сравнивается попеременно с каждым из имеющихся образцов. Затем выбирается эталон, с которым набор признаков имеющегося символа совпадает лучше всего, и на основе этого делается вывод о принадлежности этого символа к тому или иному классу. Такой подход по сути своей не позволяет добиться высокого качества распознавания, как бы он не был усовершенствован [1; 2].

Главный его недостаток заключается в том, что в любом случае в наборе признаков содержится не вся информация об изображении и вариантов изображения того или иного символа будет больше, чем эталонов. Тогда, как только система сталкивается с деформационными искажениями в структуре объекта распознавания (нестандартным написанием буквы или цифры), возникает проблема соотнесения исследуемого изображения к определенному классу объектов распознавания.

Поэтому одной из важных проблем, с которыми приходится сталкиваться при распознавании контурных изображений рукописного текста, являются различные деформационные искажения их структур, влияющие на результат распознавания [3].

Цель данной статьи – рассмотрение метода распознавания печатного и рукописного текста, устраняющего влияния различных деформационных искажений на результат распознавания.

Методы, основанные на структурном и структурно-лингвистическом подходах к распознаванию, работают в режиме реального времени и позволяют построить инвариантные признаки распознавания к различным деформационным искажениям структуры [2; 4; 5].

К деформационным искажениям можно отнести: добавление новых структурных элементов различного уровня общности по сравнению с эталонными (полученными в процессе обучения) структурами; изменение параметров структурных элементов; отсутствие в структуре распознаваемого изображения определенного класса распознавания структурных элементов, которые присутствуют в структурах эталонных (используемых в процессе обучения) изображений.

Для определения структуры распознаваемого контурного изображения, задаются базисные направления ориентации в четырех квадрантах. В каждом квадранте задается множество векторов $\bar{x}_1^{\sigma}, \bar{x}_2^{\sigma}, \ldots, \bar{x}_n^{\sigma}$. В процессе определения производных структурных элементов контура распознаваемого изображения при правом (левом) направлении обхода контура начало координат 0 совмещается с началом структурного элемента изображения. В общем случае данные построения определяют ортогональное параллельное проектирование (Pr) структурных элементов a_{ij}^n структуры Z_i^n распознаваемого изображения на вектора $\bar{X}_{\xi}^{\sigma}$ векторных пучков $\bar{X}^{\sigma}$, задающих γ-е направления ориентации $g\gamma$, $\gamma = (\overline{1, 4 \times n})$ в системе направлений ориентации X при последовательной нумерации направлений ориентации данной системы в направлении обхода контура изображения [4]:

$$Pr : a_{ij}^n \to \bar{x}_{\xi}^{\sigma} .$$

Значение функции $\underset{X}{Inv}\left(a_{ij}^n\right) = g_{\gamma}$, определяющей отображение $a_{ij}^n \to g_{\gamma}$, называется структурным инвариантом элемента a_{ij}^n структуры z_i^n в системе X.

Тогда:

$$\underset{X}{Inv}\left(z_i^n\right) = G_i^n; \quad G_i^n = \langle g, r, B \rangle,$$

где G_i^n – структура инвариантов n-го структурного уровня в системе X;

g – множество направлений ориентации в данной системе;

r – бинарные отношения, в которых находятся элементы множества A_i^n;

B – аксиомы структуры, условиям которых удовлетворяют данные отношения [5].

Выделение структуры инвариантов G_i^n на структуре z_i^n позволяет осуществить устранение влияния аффинных преобразований типа гомотетий и поворотов на процесс распознавания изображения.

Для устранения влияния деформационных искажений определяются разнородные структурные критические точки, определяющие начало формирования новой подструктуры или продолжение развития уже выявленной подструктуры.

Точки 1-го рода характеризуют продолжение развития текущей подструктуры на рассматриваемом участке контура изображения и определяют выпуклость данной подструктуры.

Точки 2-го рода характеризуют начало развития новой подструктуры на рассматриваемом участке контура изображения и определяют вогнутость подструктур.

Точки 1-го и 2-го рода описывают формирования подструктур различного уровня вложенности.

Для выделения подструктур 1-го уровня вложенности определяются:

структурные критические точки, в которых подструктура начинает свое развитие (точки максимальной вогнутости структуры);

структурные критические точки, в которых подструктура имеет пик своего развития (точки максимальной выпуклости структуры).

Максимальными структурными критическими точками 1-го рода $t_{i\ max}^1$ называются такие точки 1-го рода, которые являются потенциальными точками захвата контура изображения при сканировании бинарной матрицы значений сигналов прибора с зарядовой связью.

В данных точках структура максимально выпуклая и имеет пик развития подструктуры 1-го уровня вложенности при правом обходе контура изображения. Следующие структурные критические точки 1-го рода будут определять уменьшение развития данной выпуклой подструктуры относительно точки захвата до возникновения структурообразующей критической точки 2-го рода (точки максимальной вогнутости структуры), после которой начнется развитие следующей выпуклой подструктуры.

После выделения максимальных структурных критических точек 1-го рода определяются точки максимальной вогнутости структуры, определяющие переходы между выпуклыми подструктурами. Данные структурные критические точки являются минимальными структурными критическими точками 2-го рода. Для их определения осуществляется последовательное соединение относительно точки захвата, выделенных максимальных структурных критических точек 1-го рода отрезками, направление ориентации которых совпадает с обобщенным направлением развития данных подструктур (вогнутых подструктур, находящихся между двумя соседними максимальными критическими точками 1-го рода). Данные отрезки представляют собой новые структурные элементы $a_{i,j}^m$ m-го структурного уровня. Таким образом, строится виртуальный описанный вокруг контура изображения выпуклый многоугольник, ребра которого соответствуют структурным элементам $a_{i,j}^m$. Каждый элемент $a_{i,j}^m$ соединяет две выпуклые подструктуры 1-го уровня вложенности вогнутой структуры контура изображения, для которых необходимо найти точку максимальной вогнутости (критическую точку структурного перехода). Данные структурные критические точки будут являться минимальными критическими точками 2-го рода.

Минимальными структурными критическими точками 2-го рода $t_{i\ min}^2$ называются такие точки 2-го рода структуры контурного изображения, для которых перпендикуляры p_j, опущенные от соответствующих структурных элементов $a_{i,j}^m$ на данные структурные критические точки, будут иметь максимальную длину для соответствующих выделенных подструктур.

Построение структуры высшего уровня общности по структурным критическим точкам 1-го и 2-го рода, представленное на рисунке, имеет преимущество по сравнению с известными структурными методами распознавания контурных изображений, основанных на построении скелетонов путем разложения их контуров на ленты за счет того, что определение критических точек в предложенном подходе не связано с нахождением экстремумов кривизны, для отыскания которых необходимо явное задание кривой, что не всегда возможно [3].

Полученная обобщенная структура контурного изображения I_i образует концепт $Cpt(I_i)$ распознавания, содержащий необходимые и достаточные признаки классов объектов распознавания:

$$Cpt(I_i) = z_i^{m+1} = \left\langle A_i^{m+1},\ r,\ B \right\rangle,$$

где A_i^{m+1} – множество структурных элементов m+1 уровня общности $A_i^{m+1}\left\{a_{i1}^{m+1},\ a_{i2}^{m+1}, \ldots,\ a_{ik}^{m+1}\right\}$.

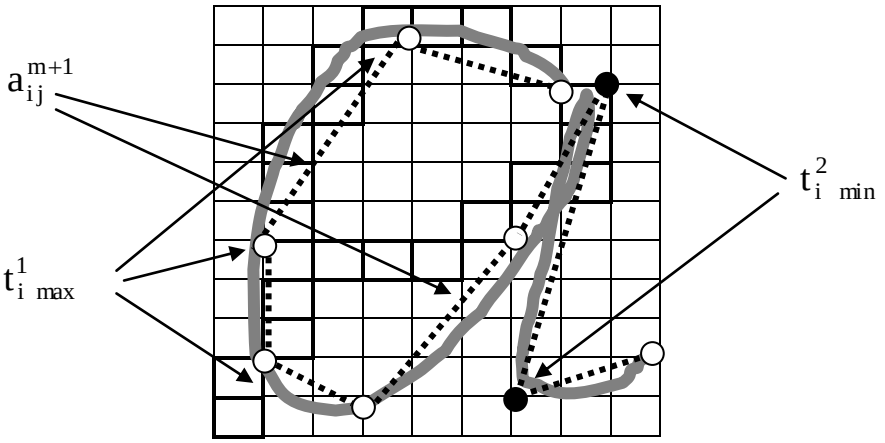


Рис. **Структурные критические точки**

○ ●

Пусть $T_{max}^{1} = \{t_{1\,max}^{1}, t_{2\,max}^{1}, \ldots, t_{n\,max}^{1}\}$, $T_{min}^{2} = \{t_{1\,min}^{2}, t_{2\,min}^{2}, \ldots, t_{m\,min}^{2}\}$.

При отображении h данных множеств T_{max}^{1} и T_{min}^{2} на общую линейную шкалу порядка P

$$h : (T_{max}^{1}, T_{min}^{2}) \to P;$$

структурные элементы a_{ij}^{m+1} образуются структурными критическими точками:

$$a_{ij}^{m+1} = f(t_{k\,max}^{1}, t_{n\,min}^{1}),$$

где f − функция построения линейного структурного элемента по двум критическим точкам, последовательно расположенным на шкале P.

Тогда $A_{i}^{m+1} = F(T_{max}^{1}, T_{min}^{2})$ и $Cpt(I_i) = \langle F(T_{max}^{1}, T_{min}^{2}), r, B \rangle$.

Построенная структура инвариантна относительно аффинных преобразований и деформационных искажений контура распознаваемого изображения.

Предложенный метод, основанный на определении признаков классов объектов распознавания по структурным критическим точкам, позволяет устранить влияние различного рода аффинных преобразований и деформационных искажений в структуре контура распознаваемого изображения на качество распознавания печатного и рукописного текста.

Литература: 1. Форсайт Д. Компьютерное зрение. Современный подход / Д. Форсайт, Ж. Понс; [Пер. с англ. – М.: Изд. дом "Вильямс", 2004. – 928 с. 2. Шапиро Л. Компьютерное зрение / Л. Шапиро, Дж. Стокман; [Пер. с англ. – М.: БИНОМ. Лаборатория знаний, 2006. – 752 с. 3. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2006. – 1072 с. 4. Гринев Д. В. Классификация и идентификация объектов с использованием структурно-лингвистического метода // Системи обробки інформації. – Харків: ХВУ. – 2004. – Вип. 11 (39). – С. 44 – 48. 5. Паржин Ю. В. Структурное распознавание изображений в реальном времени / Ю. В. Паржин, В. С. Ковальчук, Д. В. Гринев // Збірник наукових праць. – К.: ІПМЄ. – 2004. – Вип. 25. – С. 143 – 147.

УДК 681.3

Пашковський В. В.

МЕТОДИКА ФОРМУВАННЯ УЗАГАЛЬНЕНОГО КРИТЕРІЮ ЗА СУКУПНІСТЮ КІЛЬКІСНИХ ТА ЯКІСНИХ ПОКАЗНИКІВ

У загальному випадку задача раціонального вибору типів, кількості засобів відображення інформації та інформаційної моделі є задачею багатокритеріальної оптимізації, тому постає необхідність у виборі методу розв'язання багатокритеріальних задач [1; 2].

З формальної точки зору, вибір найкращого варіанта інформаційного забезпечення станції радіомоніторингу є питанням прийняття рішення, що можливо подати у вигляді послідовності наступних задач:

формування множини припустимих рішень X;

вибір та обґрунтування системи оцінок, які дозволяють встановити на множині X відношення порядку (задача оцінювання);

визначення найкращого рішення $x_{opt} \in X$ (задача оптимізації).

Центральною з перерахованих задач виступає задача оцінювання. Труднощі її розв'язання полягають у тому, що в більшості випадків при синтезі, наприклад, складних інформаційно-управляючих систем не вдається вибрати єдиний показник, який досить повно характеризує систему. У зв'язку з цим виникає необхідність:

1) формувати множину часткових показників, які досить повно виражають усі значущі характеристики системи;

2) вибирати на множині часткових показників − метрики, яка дозволить встановлювати на множині рішень $x \in X$ відношення порядку.

Теоретичною основою формування багатокритеріальних скалярних оцінок є теорія корисності, яка передбачає існування кількісної оцінки переважання рішень. Це означає, що якщо рішення $x_1, x_2 \in X$ та $x_1 \succ x_2$ (x_1 переважає x_2), то $P(x_1) \succ P(x_2)$, де $P(x_1)$, $P(x_2)$ − функції корисності.

Тобто корисність є кількісною мірою "якості" рішень. У зв'язку з цим виникає задача обґрунтування правила (метрики), за яким формується функція корисності в просторі часткових критеріїв $k_i(x)$:

$$P(x) = G[k_i(x)], \; i = \overline{1,n}. \qquad (1)$$

Синтез будь-якої математичної моделі, в тому числі й синтез функції корисності, передбачає необхідність вирішення двох взаємопов'язаних задач: структурної та параметричної ідентифікації. Перша з них передбачає:

визначення значущих факторів, які впливають на вихідні дані моделі;

визначення структури, тобто вигляду оператора, який установлює зв'язок між вхідними та вихідними даними моделі.

Рішення задачі полягає у визначенні кількісних та якісних значень показників засобів відображення інформації, що пов'язано з висуванням та перевіркою деякої гіпотези. В розглянутому випадку вигляд функції корисності рішення X визначається частковими характеристиками (критеріями) $k_i(x)$ та в загальному випадку ці характеристики різнорідні й мають різноманітні "ваги" для особи, яка приймає рішення.

Це означає, що формула (1) може бути записана у вигляді:

$$P(x) = F[\lambda_i, k_i(x)], \; i = \overline{1,n}, \qquad (2)$$

де λ_i − коефіцієнт важливості i -го часткового показника $k_i(x)$;

F − оператор, який визначає вигляд залежності.

Раціональне рішення за багатьма частковими показниками включає: нормалізацію часткових показників з метою приведення їх до єдиного інтервалу вимірювання, однієї розмірності (безрозмірного вигляду); формування узагальненого показника; знаходження оптимального рішення.

Для нормалізації часткових якісних показників пропонується використати ідеї теорії нечітких множин, а для часткових кількісних показників − вагові коефіцієнти, отримані на основі обробки експертної інформації [1; 2].

Найбільш повний критичний огляд сучасних методів рішення багатокритеріальних задач наведений у роботах [3; 4]. У практичній діяльності перевага надається методам експертних оцінок або безпосередньо відповідальним керівникам − особам, що приймають рішення. Колективна думка групи досвідчених спеціалістів-експертів є рекомендацією для особи, що приймає рішення. Переваги, які встановлюються при цьому, ґрунтуються на великому досвіді та знаннях експертів і особи, що приймає рішення, та, як показує багаторічна практика, приводять у більшості випадків до успіху. Перелік найбільш відомих у теперішній час методів [1] виглядає наступним чином:

а) метод узагальнених критеріїв;

б) метод ELECTRE;

в) лексикографічні методи (метод послідовних поступок);

г) метод результуючого показника якості;

д) послідовна оптимізація;

е) непідкорені альтернативи.

Метод узагальнених критеріїв, у свою чергу поділяється на: метод числових значень; метод вибору одного з критеріїв; адитивний метод; мультиплікативний метод; комбінація адитивного та мультиплікативного методів.

Метод ELECTRE ґрунтується на побудові графа переваги за кожним критерієм оптимальності. Потім за допомогою спеціальних прийомів та додаткової інформації будується узагальнений граф і знаходиться рішення, яке є кращим.

Суть лексикографічних методів (метод послідовних поступок) полягає у виділенні спочатку множини альтернатив з найкращою оцінкою за найбільш важливим показником. Якщо така альтер-

натива одна, то вона приймається найкращою, а якщо їх декілька, то з їх підмножини виділяють ті, котрі мають найкращу оцінку за другим за важливістю показником, і т. д.

Для розширення множини розглянутих альтернатив та покращення якості рішення за сукупністю показників може призначатися поступка, в межах якої альтернативи вважаються еквівалентними.

Принципіальною особливістю розглянутої задачі вибору рішення є як кількісний, так і якісний характер критеріїв. У зв'язку з цим розглянуті методи багатокритеріальної оптимізації повинні формулюватися в нечіткій постановці.

Метод результуючого показника якості ґрунтується на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу часткових показників якості $q_1,\ldots q_m$ на результуючу якість виконання системою її функцій. Оцінки такого впливу даються групою спеціалістів-експертів, що мають досвід розробки подібних систем.

Переважна більшість методів ґрунтується на формуванні тим чи іншим чином з часткових критеріїв системи узагальненого критерію, який потім максимізується (мінімізується). За допомогою такого прийому багатокритеріальна задача зводиться до однокритеріальної.

Найбільше застосування серед результуючих критеріїв отримали максимінний, адитивний та мультиплікативний критерії. Розглянемо більш детально кожен з них.

Максимінний критерій забезпечує найкраще (найбільше) значення найгіршого (найменшого) з часткових показників якості.

У ряді випадків вид результуючої цільової функції досить важко обґрунтувати або застосувати. В подібних випадках можливим простим шляхом розв'язання задачі є застосування максимінного показника. Правило вибору оптимальної системи Z у цьому випадку має наступний вигляд:

$$\max_{Z\in M_z}\ \min_{1\le j\le m}\ \{\overline{q_1}(Z),\ldots,\overline{q_j}(Z),\ldots,\overline{q_m}(Z)\},$$

якщо вагові коефіцієнти часткових показників відсутні;

$$\max_{Z\in M_z}\ \min_{1\le j\le m}\ \{\overline{q_1}^{w_1}(Z),\ldots,\overline{q_j}^{w_j}(Z),\ldots,\overline{q_m}^{w_m}(Z)\},$$

якщо вагові коефіцієнти визначені.

Адитивний критерій містить у собі суму зважених нормованих часткових показників та має наступний вигляд:

$$P_j=\sum_{i=1}^{n}\lambda_i k_{ij}\ , \qquad (3)$$

де k_{ij} – нормоване значення j-го показника;

λ_i – ваговий коефіцієнт j-го показника.

Головним недоліком адитивного показника є те, що при його застосуванні може відбуватися взаємна компенсація часткових показників. Це означає, що зменшення одного з показників може бути компенсоване збільшенням іншого показника. Для послаблення цього недоліку вводяться спеціальні обмеження на мінімальне значення часткових показників та їх вагові коефіцієнти.

Мультиплікативний показник утворюється за допомогою перемноження часткових показників з урахуванням вагових коефіцієнтів та має вигляд:

$$P_j=\prod_{i=1}^{n}k_{ij}^{\lambda_i}\ . \qquad (4)$$

Найбільш суттєва відмінність мультиплікативного показника від адитивного полягає в тому, що адитивний показник базується на принципі справедливої абсолютної поступки за окремими показниками, а мультиплікативний – на принципі справедливої відносної поступки. Справедливим вважають такий компроміс, коли сумарний рівень відносного зниження одного або декількох показників не перебільшує сумарного рівня відносного збільшення решти показників.

Стосовно задачі вибору раціонального варіанта інформаційного забезпечення станції радіомоніторингу запропоновано врахування максимальної кількості часткових показників інформаційного забезпечення станції радіомоніторингу. А саме врахування кількісних та якісних показників з їх ваговими коефіцієнтами та отримання узагальненого адитивного показника з обмеженнями на мінімальні значення часткових показників і їх вагові коефіцієнти.

Для випадку, коли показники подані в якісному вигляді, пропонується побудова функцій належності заданого рівня якості та визначення кількісних значень відповідних значень часткових показників залежно від варіанта інформаційного забезпечення та його конкретного якісного показника:

$$W=\sum_{j=1}^{e}w_j\cdot q_j+\sum_{j=e+1}^{m}w_j\cdot\mu_j\ ,$$

де e – число кількісних показників;

$m-e$ – число якісних показників.

Вибравши метод розв'язання багатокритеріальної задачі та врахувавши кількісні і якісні часткові показники, створюється передумова переходу до розробки методичного апарату вибору раціонального варіанта інформаційного забезпечення станції радіомоніторингу.

Література: 1. Адаменко А. Н. Информационно-управляющие человеко-машинные системы: Исследование, проектирование, испытания: Справочник / А. Н. Адаменко, А. Т. Ашеров, И. Л. Бердников. – М.: Машиностроение, 1993. – 528 с. 2. Шибанов Г. П. Количественная оценка деятельности человека в системах человек-техника. – М.: Машиностроение,1983. – 264 с. 3. Герасимов Б. М. Эргономический анализ деятельности оператора автоматизированных систем / Б. М. Герасимов, Б. М. Егоров, А. В. Линник. – К.: КВИРТУ ПВО, 1979. – 160 с. 4. Суходольский Г. В. Структурно-алгоритмический анализ трудовой деятельности. – Л.: ЛГУ, 1976. – 128 с.

Podbregar I.

Brumnik R.

УДК 004.738.5:343.326

COMPUTER ATTACKS AND GLOBAL TERRORISM

It is problematic defining a "Cyberattack" such as "Cybercrime" or "Cyberterrorism" cause of difficult determining with certainty the identity, intent, or the political motivations of an attacker. Often we equated simple use of malicious code with "Cyberterrorism" which usually involve more factors like just a computer hack. However, a "Cyberterrorism" event may also sometimes depend on the presence of other factors beyond just a "Cyberattack."

There are many different definitions exist for the term "Cyberterrorism" like as many definitions exist for the term "Terrorism" (Under 22 USC, Section 2656, "terrorism" is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The United States has employed this definition of terrorism for statistical and analytical purposes since 1983. U. S.) [1]. Security expert Dorothy Denning [2; 3] defines Cyberterrorism as "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage". Some definitions of Cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" [4].

Others definitions indicate such as physical attacks that destroy computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard, also be labeled as Cyberterrorism [5]. Thus, it is possible that if a computer facility were deliberately attacked for political purposes, all the methods described above (physical attack, Cyberattack) might contribute to, or be labeled as "Cyberterrorism".

Business, government and industry have all become addicted to information. Theirs depends of information creates opportunities for terrorism. Computer and information security, data protection, and privacy are all growing problems. No single technology or product will eliminate threats and risk. Securing our computers, information, and communications networks secure our economy and our country. A global strategy and policy for combating this type of terrorism is need now.

It is necessary to know that these methods of terror, producing destruction, and fear can be much more destructive online than other conventional methods in the real world.

To avoid much malicious possibility it is today's research and development task to produce the crime-resistant products of the future. So we must take every opportunity we can to use science and technology to reduce crime and improve the quality of our lives. In this article we focused on different aspects of "Cyberterrorism", their begin fundamentals and against fights methods.

Netwar Overview

Where is cybercrime today? Where it is headed? Espionage? Botnets? Trojans? Spyware? Denial-of Service attacks? Phishing scams? Zero-day exploits (Computer code that exploits a vulnerability for which a patch is not yet available)? The reality is that no one is immune from this malicious industry's reach — individuals, businesses, even governments. Many sophisticated computer technologies are developing in new era. Also there are growing dangers from crimes committed against information on computers, or against computers. In most countries around the world, however, existing laws are likely unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforcing. As cyber crime increasingly breaches national borders, national governments should examine their current statutes to determine whether they are sufficient to combat the kinds of crimes discussed in this article. Where

gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes. Many reports describe about possible effects of a coordinated Netwar against the most critical infrastructure. Also there are many discussions about open options to extremists, or terrorist groups for obtaining malicious technical services from cybercriminals to meet political or military objectives.

Cyberattack, Cybercrime, Cyberterrorism

A great deal of "cracks" are committed for the purposes of anarchy, humor, or as often stated by the perpetrators, "to be annoying". However, is this the mindset of a cyberterrorist? Does he change an web site to say a country's government is evil? Does he hack into a major corporation's voice mail system to make long distance calls? No, that isn't domain of the cyberterrorist. That is domain of the amateur cracker demonstration. A cyberterrorist will disrupt the banks, the international financial transactions, the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a cyberterrorist attempt to gain entry to the goverment building or equivalent? Likely, since arrest would be immediate. However, in the case of the cyberterrorism, the perpetrator sitting on another continent while a nation's economic systems grind-down. Destabilization will be achieved.

What's New In Netwar?

Undeterred by the prospect of arrest or prosecution, cybercriminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nation's security. Headlines of Netwar attacks command our attention with increasing frequency. Moreover countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities the potential for copycat crimes and the loss of public confidence. Sophisticated tools for cyberattack we can found for sale or freeware on the web. Highly-organized underground cybercrime businesses host websites advertise a variety of disruptive software products and malicious technical services.

High-end cybercrime groups use standard software business development techniques to keep their products updated with the latest antisecurity features. Also they seek and recruit new and talented software engineering students into their organizations. As in next chapter shows the laws of most countries do not clearly prohibit cybercrime.

Problem to Cybercrime definition harmonize

Cybercrime can be very broad in scope and may sometimes involve more factors than just a computer hack. Cyberterrorism is often equating with using of malicious code. However, a cyberterrorism event may also sometimes depend on the presence of other factors beyond just a cyberattack.

Problem of transitional nature of Cybercrime

Effective law providing is complicate cause of transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cybercrime. However, the future of the networked world demands a more proactive approach, whereby governments, industry, and the public work together to devise effective laws that will effectively determined cyber criminals. "Fighting cybercrime is a 24/7 battle, a global battle, and it is far from over" (DeWalt, 2007).

It is easy to learn how to commit; they require few resources relative to the potential damage caused they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

Problem to international Law harmonize

Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national. New technologies continue to outpace policy for law enforcement. Problems of coordination among agencies of different countries, along with conflicting national policies about crime in cyberspace, work to the advantage of cybercriminals who can choose to operate from geographic locations where penalties for some forms of cybercrime may not yet exist. boundaries, or designing attacks that appear to be originating from foreign sources. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Outdated laws may not cover web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks as protected forms of property.

Ethics and moral doubts

Over the past 10 years, crime has been moving away from stealing physical goods, towards obtaining information. First the means of robbery changed to keep up with an age where people carry identity information in the form of credit cards instead of cash. However, these are just the modern equivalents to common mugging.

Recently though, whole new information markets have opened up as playing fields for computer criminals. Much of the internet economy revolves around advertising. And much of this advertising is targeted by using databases of personal information. This information is extremely valuable, and could be stolen, and a black market of information created. Information such as medical records, HIV test results, and personal emails could all be stolen and sold to advertisers and other information-based companies.

One of the most worrying is the terrorists moving online, and engaging in what is called cyber-terrorism. These methods of producing destruction, terror, mayhem, and fear can be much more destructive online than other conventional methods in the real world.

What types exactly will depend on what new forms of security tomorrow's criminals will need to break. Will people be synthesizing voice authorizations? Or running replay attacks on retinal scanners? Or even learning to imitate a victim's typing style. All we can be sure of, is that criminals of tomorrow, like those of last century and those of today, will keep on innovating.

Netwar – War of the future

Cyber espionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files. However, should a terrorist group, nation, or other organization use computer hacking techniques for political or economic motives. Their deliberate intrusions may also qualify them, additionally, as cybercriminals. If there is disagreement about this, it is likely because technology (figure) has outpaced policy for labeling actions in cyberspace. In fact, industrial cyber espionage may now be consider a necessary part of global economic competition, and secretly monitoring the computerized functions and capabilities of potential adversary countries may also be consider essential for national defense.

ECHELON is a name used in global media and in popular culture to describe a signals intelligence collection and analysis network operated on behalf of the five signatory states to the UKUSA agreement; Australia, Canada, New Zealand, the United Kingdom and the United States, known as AUSCANZUKUS. ECHELON was capable of interception and content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission, public switched telephone networks and microwave links.

The UKUSA intelligence community is assessed by the European Parliament to include the Signals Intelligence organizations of each of the member United States National Security Agency, United Kingdom Government Communications Headquarters, Canada Communications Security Establishment, Australia Defence Signals Directorate and New Zealand Government Communications Security Bureau. The EP report concludes that it seems likely that ECHELON is a method of sorting captured signal traffic, rather than a comprehensive analysis tool.

Figure. **Diagram of Purported Echelon Spy System**

U. S. counterintelligence officials reportedly have stated that about 140 different foreign intelligence organizations regularly attempt to hack into the computer systems of U. S. government agencies and U. S. companies. Cyber espionage, which enables the ex-filtration of massive amounts of information electronically, has now transformed the nature of counterintelligence.

Satan

SATAN features an easy-to-use interface, an extensible framework, and a scaleable approach to checking systems. First, the user interface consists of HTML pages that are used through a Web browser such as Mosaic or Netscape.

SATAN is an automated network vulnerability search and report tool that provides an excellent framework for expansion. The authors indicate that SATAN stands for "Security Analysis Tool for Auditing Networks".

Kerberos

KERBEROS model is based on a trusted third-party authentication protocol. The original design and implementation of Kerberos was the work of MIT Project Athena staff members. Kerberos is publicly available and has seen wide use.

Kerberos is a network authentication system developed at MIT to address this problem. It enables users communicating over networks to prove their identity to each other while optionally preventing eavesdropping or replay attacks. It provides data secrecy using encryption. Kerberos provides real-time authentication in an insecure distributed environment.

How avoid to unexpected scenarios?

To avoid many malicious possibilities it is today's research and development task to produce the crime-resistant products of the future. So we must take every opportunity we can to use science and technology to reduce crime and improve the quality of our lives.

In order for a wide implementation of this technology, standards must be developed that will allow for their consistent use. The International Organization for Standards ISO/IEC JTC1 is the governing body of international biometric standards, but this standardization is still in progress. Also there are many International Standards such us ISO/IEC 19794-5 to define Image Quality Requirements and BS7799 covering ten major sections, each a different area as a Business Continuity Planning, System Access Control, System Development and Maintenance, Physical and Environmental Security, Compliance, Personnel Security, Security Organisation, Computer & Network Management, Asset Classification and Control, Security Policy to maximum protect Information System and personal informations.

In the future, fixed biometric standards will be in place to guide vendors and developers in the areas of biometric application profiles, interfaces, and system performance. Along with standardization there should be certain privacy issues addressed by law such as privacy and specific use guarantees as well as checks and balances to conduct audits to ensure compliance with these guarantees. This is a good reason that encryption and digitalization are recommended by leading industry organizations such as International Biometrics Industry Association (IBIA) and the BioAPI Consortium.

Conclusion-Future Challenges

Global security trend identified by security experts consulted is the emergence of an entire economy geared to outfit criminals with the tools for cybercrime.

Reliance on terrestrial laws is an untested approach

Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber crimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.

Weak penalties limit deterrence

The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.

Self-protection remains the first line of defense

The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

A global patchwork of laws creates little certainty

Little consensus exists among countries regarding exactly which crimes need to be legislated against. In the networked world, no island is an island. Unless crimes are define in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cybercrime will be complicated.

A model approach is need

Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for ecommerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens.

Literature: 1. http://www. state. gov/s/ct/rls/pgtrpt/ 2001/html/10220.htm 2. Dorothy Denning. Activism, Hactivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy / John Arquilla and David Ronfeldt, eds. – Networks and Netwars, Rand 2001. – P. 241. 3. Dorothy Denning. Is Cyber War Next? // Social Science Research Council, November 2001. – http://www. ssrc. org/sept11/essays/denning. htm. 4. http://www. fema. gov/pdf/onp-/toolkit_app_d. pdf 5. Dan Verton. A Definition of Cyber-terrorism // Computerworld. – August 11, 2003. – http://www. computerworld. com/securitytopics /security/story /0,10801,83843,00. html 6. Europol: Computer-related crime within the EU: Old crimes new tools; new crimes new tools. – Luxembourg: Office for Official Publications of the European Communities, 2003. 7. Hicklin R. A. The Role of Data Quality in Biometric Systems / R. A. Hicklin, R. Khanna (2006). 8. Jain A. K. BIOMETRICS: Personal Identification in Networked society / A. K. Jain, R. Bolle, S. Pankanti. – Kluwer Academic Publishers (1999). 9. Janbandhu P. K. Novel biometric digital signatures for Internet-based applications / P. K. Janbandhu, M. Y. Siyal (2001) // Management and Computer Security. – 2001. – Vol. 9. 10. Maltoni D. Handbook of Fingerprint Recognition, Springer Verlag / D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar (2003). 11. Mitnick D. Kevin The Art of Deception: Controlling the Human Element of Security. – Indianapolis: John Wiley & Sons Inc. 2002. 12. Nadel L. On the Future of Biometrics – Research, Applications, and Social Challenges, IEEE CVPR 2006. 13. National Institute of Standards and Technology, (1993): Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-2 (1993). 14. Pocar Fausto. New Challenges for International Rules against Cyber-Crime // European Journal on Criminal Policy and Research. – 2004. – Vol. 10. – No. 1. – P. 27 – 37. 15. Ratha N. K. An analysis of minutiae matching strength / N. K. Ratha, J. H. Connell, R. M. Bolle. – Proc. 3rd AVBPA. – Halmstad, Sweden, 2001. 16. Umut Uludag Multimedia Content Protection Via Biometrics-Based Encryption International Conference on Multimedia and Expo (ICME 2003) / Uludag Umut, K. Jain Anil. – Baltimore, Maryland, USA.– 2003. 17. Wilson C. CRS Report for Congress, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. – Washington, 2008.

Куркін М. В.

УДК 330.115:658.1

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Процеси взаємодії вітчизняних підприємств із зовнішнім середовищем протікають в умовах недостатньо розвиненої ринкової інфраструктури, правового нігілізму суб'єктів господарювання, різких коливань ринкового попиту, високої динаміки змін у правовому просторі економіки, що істотно підвищує рівень загроз економічній безпеці суб'єктів господарювання. У зв'язку з цим у теоретичних і прикладних дослідженнях сучасної економічної науки все частіше постає проблема забезпечення економічної безпеки розвитку підприємства. У цьому зацікавлена й держава, інтерес якої до безпечної діяльності підприємств диктується, насамперед, необхідністю забезпечення її економічної незалежності й цілісності, а також підвищенням політичного, економічного та соціального статусу на міжнародній арені. Суб'єкти господарювання, у свою чергу, прагнуть забезпечити власні інтереси, які проявляються в прагненні до збереження й збільшення капіталу, що в сучасних умовах конкурентної боротьби вимагає використання спеціального арсеналу інструментів (методів і засобів), що чутливо реагують на невизначеність зовнішнього середовища й адаптації до цих економічних умов внутрішньої організаційно-управлінської системи.

Вивчення присвячених питанням забезпечення економічної безпеки наукових праць [1 – 5] дозволило визначити кілька етапів у розвитку цього напрямку організаційно-управлінської діяльності підприємств. Так, на першому етапі проблема в основному зводилася до збереження й захисту комерційної таємниці та інших секретів підприємства. На другому етапі акцент проблеми безпеки діяльності суб'єктів господарювання був перенесений на організацію захисту від впливу зовнішнього середовища й адаптації до її стану.

Ряд сучасних дослідників дотримуються ресурсно-функціонального підходу до забезпечення економічної безпеки підприємств [6; 7], розглядаючи її як "...стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз та забезпечення стабільного функціонування в даний час і у майбутньому" [8, с. 138].

У сучасних російських періодичних виданнях, присвячених проблемам безпеки функціонування бізнес-структур, значне місце приділяється проблемі захисту інформації й кадрів (персоналу) [4; 9]. Останні характеризуються як особливий фактор – джерело розголошення комерційної таємниці. Інформація й розширення комунікативних зв'язків підприємства – це особливий аспект проблеми організації економічної безпеки діяльності підприємств, що з'явився на порядку денному.

За результатами розвитку підприємство закономірно стає більш відкритою системою, оскільки зростає число каналів взаємозв'язків підприємства з зовнішнім середовищем, змінюються й ускладнюються комунікативні зв'язки. Це збільшує обсяг й інтенсивність зовнішніх потоків інформації. Одночасно об'єктивно ускладнюється система внутрішніх взаємозв'язків та інформаційних потоків, що вимагає зміни й внутрішньої організаційної структури підприємства.

До об'єктів, що входять у систему обмінних комунікативних зв'язків підприємства в процесі розвитку виробничо-господарської діяльності й формують його загрози, варто віднести, насамперед, потоки інформації, інвестиції й фінансування, поставки товарно-матеріальних цінностей, придбання нових технологій, патентів, ліцензій, залучення кваліфікованого персоналу.

Система управління економічною безпекою повинна забезпечувати захищеність усіх комунікаційних каналів і трансакцій, пов'язаних з організацією, зберіганням, передачею, виробництвом та відтворенням інформаційних ресурсів підприємства і їх похідних на всіх рівнях управління підприємством.

Усі процеси, пов'язані з організацією безпеки, розподіляються на процеси безпечного розвитку інформаційних властивостей і властивостей інформаційних ресурсів. При цьому визначається основна (базова) властивість, що є переважаючою для суб'єкта рівня управління підприємством. Як початкові властивості розглядаються об'єктивність, вірогідність, адекватність, своєчасність, коректність, точність і корисність. Процеси розвитку пов'язуються з розвитком цих властивостей суб'єктами різних рівнів управління підприємством. Практична реалізація безпечного розвитку здійснюється відповідно до стандарту економічної безпеки й посадових повноважень (інструкцій).

Дієвість системи управління економічною безпекою підтверджується категоріями інформаційної безпеки, такими, як конфіденційність, цілісність, доступність компонентів інформаційних ресурсів підприємства на всіх рівнях управління підприємством. Дані категорії визначають властивості, що відносяться до положень захищеності інформації й інформаційних систем [10; 11]. Використання цих понять дозволяє сформулювати безпечні режими роботи з інформацією і визначає ефективність засобів захищеності інформаційних ресурсів інформаційної системи (ІС), що експлуатується на підприємстві.

Застосування системного підходу до організації процесів забезпечення інформаційної безпеки підприємства на основі положень теорії інформації, уточнення поняття інформаційного ресурсу та визначення ІС як підтримуючої системи щодо інформаційних ресурсів – найважливіше завдання підвищення ефективності інформаційної безпеки підприємства [12].

Під інформацією будемо розуміти множину даних, кожна підмножина яких характеризується такими властивостями: об'єктивність, вірогідність, адекватність, своєчасність, коректність, точність, корисність, цінність. У різних літературних джерелах із зазначеної множини властивостей виділяють тільки певну частину з них, керуючись, у першу чергу, винятково практичними міркуваннями. Так, наприклад, властивості адекватності й вірогідності об'єднують в одну – вірогідності; об'єктивності та коректності – у властивість об'єктивності й т. д. Проаналізуємо решту властивостей – своєчасність, точність, корисність і цінність. Очевидним є той факт, що визначальною є властивість корисності, яка свідчить, що інформація повинна бути точною та своєчасною. Таким чином, можна висловити базове твердження, що властивість інформації певною мірою характеризує певну функцію управління, реалізовану суб'єктом, який використовує інформацію, що приводить до наступної системи тверджень.

Твердження 1. Інформація, що використовується суб'єктом щодо якої-небудь дії, повинна реалізувати (виконувати) певну функцію суб'єкта в системі (структурі) управління підприємством. Як такі функції можна розглядати функції управління, управління виробництвом, прийняття рішень, планування й т. д.

Унаслідок того, що реалізована функція управління визначається рівнем управління і відповідних функцій суб'єкта управління, можна припустити, що потреба в інформації, в першу чергу, визначається тією її властивістю (або ж сукупністю властивостей), яка вважається основною у процесі її використання.

Твердження 2. Для ефективної реалізації своєї управлінської функції суб'єктові необхідно розвивати кількісні на якісні характеристики тієї властивості, яка є основною, обов'язковою, такою, що часто використовується (або ж групи властивостей).

Як наслідок, з нього випливає:

Твердження 3. Безпека розвитку інформаційних ресурсів визначається безпекою розвитку тих властивостей інформації, які є визначальними для суб'єкта, рівнем управління, характером розв'язуваних завдань і, як наслідок, змістом посадових інструкцій, існуючою схемою документообігу.

Наведені твердження передбачають базування управлінських рішень і дій на концепції інформаційної безпеки, основними положеннями якої є такі:

1) розвиток інформаційних ресурсів розглядається як сукупність процесів, процедур, окремих операцій, що забезпечують розвиток різних властивостей інформації;

2) безліч властивостей інформації визначається рівнем управління й, відповідно, тими завданнями, які, в першу чергу, вирішуються суб'єктом у процесі його діяльності з досягнення цілей;

3) безпека інформаційних ресурсів визначається рівнем управління й безпекою розвитку тих властивостей інформації, які є базовими для даного рівня управління підприємством;

4) безпека інформаційної системи визначається безпекою функціонування її підсистем і компонентів, які забезпечують конфіденційність, цілісність, доступність інформації на всіх рівнях управління підприємством;

5) основна функція ІС – забезпечення (забезпечувальна підсистема) безпечного розвитку властивостей інформації на всіх рівнях управління підприємством.

Отже, ІС виступає як інструментальний засіб (сукупність засобів), який забезпечує безпечний розвиток властивостей інформаційних ресурсів на всіх рівнях управління підприємством.

Оптимальний стан відповідності категорій безпеки ІС і властивостей інформації подано в табл. 1.

Таблиця 1

Властивості інформації й визначення категорій безпеки ІС

Властивості інформації	Категорії безпеки, що забезпечуються ІС		
	конфіденційність	цілісність	доступність
Об'єктивність	+	+	+
Вірогідність	+	+	+
Адекватність	+	+	+
Своєчасність (оперативність)	+	+	+
Коректність	+	+	+
Точність	+	+	+
Корисність	+	+	+
Цінність	+	+	+

У табл. 1 знаком "+" визначені ті властивості інформації, які забезпечуються категоріями безпеки ІС.

Наведені властивості інформації мають повноту з погляду їхнього забезпечення і досяжності всіма категоріями захисту з боку ІС. Однак на практиці зазначена ситуація не відповідає можливим потенційним ситуаціям або ж не може скластися через цілий ряд обставин. Припустимо, що для

кожного рівня управління підприємством повинні виконуватися вимоги мінімального забезпечення захищеності властивостей інформації відповідними категоріями захисту з боку ІС. Тоді вихідну табл. 1 можна декомпозувати на безліч таблиць, які характеризують захищеність різних рівнів управління підприємством.

Для цього виділимо наступні основні відношення між властивостями інформації, наведені в табл. 1: об'єктивність – доступність; вірогідність – конфіденційність; адекватність – конфіденційність, цілісність, доступність; своєчасність – доступність; коректність – цілісність, доступність; точність – доступність, конфіденційність; корисність – конфіденційність, цілісність, доступність; цінність – конфіденційність, цілісність, доступність. Таким чином, табл. 1 зведемо до вигляду табл. 2.

Таблиця 2

Базова конструкція забезпечення властивостей інформації категоріями захисту

Властивості інформації	Категорії безпеки, що забезпечуються ІС		
	конфіденційність	цілісність	доступність
Об'єктивність			+
Вірогідність	+		
Адекватність	+	+	+
Своєчасність (оперативність)			+
Коректність		+	+
Точність	+		+
Корисність	+	+	+
Цінність	+	+	+

В аспекті розвитку економічних відносин важливе місце займають ІС підприємств, що виступають як інформаційний компонент системи управління підприємством. Подання ІС у вигляді сукупності власне даних, інформації та різних продуктів, породжених нею, методів і засобів її організації, зберігання, а також маніпулювання ними, обробки, аналізу, підходів до вироблення управлінських рішень вимагає розробки методик підвищення стабільності ІС підприємства у двох аспектах: стабільності протікання процесів, стабільності функціонування програмно-апаратних засобів і психологічної стабільності персоналу. З погляду інформаційної безпеки, підвищення стабільності ІС може розглядатися як мінімізація ризиків завдання збитків її підсистемам, компонентам та елементам у результаті навмисних або ненавмисних дій з боку суб'єктів (внутрішніх і зовнішніх), які беруть участь у процесах, що відбуваються в ІС, або ж запобігання завданню збитків за рахунок розробки та проведення відповідних заходів щодо захисту всіх елементів і процесів, які забезпечують функціонування ІС.

Аналіз досліджень у цій сфері показав, що на даний момент відсутній комплексний підхід до забезпечення безпеки ІС: так, наприклад, деякі автори розглядають ІС як сукупність елементів інформаційної інфраструктури, причому з метою забезпечення її безпеки для кожного з елементів розробляються своя модель, методи й засоби захисту [13]. Цей підхід відрізняється тим, що інформаційна інфраструктура характеризується безліччю процесів, що безпосередньо відносяться до формування й обробки інформації, комунікаційними зв'язками (відносинами) з елементами організаційної структури, персоналом, різними суб'єктами, що використовують інформацію, і т. п. [13]. Ці елементи самі індукують інформацію на підприємстві, що, у свою чергу, призводить до значного збільшення її обсягу, складності і вимагає впорядкованості для підвищення рівня задоволення нею потреб користувачів. У зв'язку з цим виникає проблема фільтрації так називаного "інформаційного шуму" – інформації та відомостей, які є надлишковими, неактуальними, різнорідними, такими, що перешкоджають використанню інформації, що є найбільш релевантною для вирішення проблеми або задачі в сформованій ситуації.

Іншим завданням є розробка методів підвищення стабільності ІС підприємства на основі мінімізації ризиків, пов'язаних із завданням збитків як діяльності підприємства, так і його інформаційній інфраструктурі, та підвищення стабільності всіх інформаційних процесів, включаючи методи і засоби одержання, введення, обробки та аналізу інформації.

Для вирішення цього завдання сформулюємо наступні положення:

об'єктами забезпечення інформаційної стабільності є інформаційні процеси, інформаційні продукти, отримані в процесах перетворення інформації, та інформаційна інфраструктура підприємства в цілому;

стабільність інформаційних процесів визначається збереженням усіх властивостей інформації й інформаційних продуктів, створених у процесі життєвого циклу інформаційних продуктів (ЖЦ ІП);

ЖЦ ІП характеризується часовим обмеженням, тривалість якого визначається тривалістю етапів їхнього формування, становлення й розвитку;

безпека і підвищення стабільності інформаційного продукту забезпечується сукупністю засобів захисту на всіх етапах його життєвого циклу;

засоби захисту існуючої інформаційної інфраструктури підприємства базуються на засобах захисту, що використовуються в тих процесах, які пов'язані зі зберіганням, введенням, модифікацією й передачею інформації за умови збереження всіх її властивостей;

засоби захисту забезпечують захист інформаційного продукту на всіх етапах його життєвого циклу.

Стабільність інформаційних процесів визначається збереженням і забезпеченням властивостей інформації на етапах ЖЦ ІП:

формування – обмеження доступу до первинної інформації, введення даних, операцій модифікації, коректування, зберігання;

становлення – обмеження доступу до процесів обробки, результатів попередньої обробки; експертиза й верифікація оброблених даних, внутрішній аудит отриманих інформаційних продуктів;

розвиток – обмеження доступу до аналітичної інформації, що має стратегічний характер, конфіденційний доступ до стратегічних сховищ даних, обмеження доступу до використання аналітичних інструментів.

Таким чином, запропонований метод зводиться до визначення етапів створення інформаційного продукту і формування відповідних засобів захисту на рівні обмеженого доступу до аналітичної інформації. Останнє становить *функцію управління обмеженням доступу до конфіденційної і стратегічної інформації.*

Забезпечення безпеки стадій ЖЦ ІП визначається захищеністю засобів взаємодії в процесі створення інформаційних продуктів користувачами на всіх його етапах.

У табл. 3 наведені типи взаємодій, їх характер і засоби захисту інформації на всіх етапах ЖЦ ІП.

Таблиця 3

Етапи життєвого циклу і засоби захисту інформаційного продукту

Етап ЖЦ ІП	Вид взаємодії	Засоби захисту
Формування	Доступ, підготовка	Обмеження доступу до первинної інформації, введення даних, операцій модифікації, коректування, зберігання
Становлення	Доступ, обробка	Обмеження доступу до процедур обробки, результатів попередньої обробки, експертиза й верифікація оброблених даних, внутрішній аудит
Розвиток	Доступ, аналіз	Обмеження доступу до аналітичної інформації, що має стратегічний характер, доступ до стратегічних сховищ даних, використання аналітичних інструментів

Основна ідея використання ЖЦ ІП полягає в тому, що стабільність інформаційних продуктів на нижчих рівнях управління підприємством повинна зберігатися протягом більш тривалого проміжку часу (мати більш тривалі стадії формування й становлення), а на вищих рівнях – менш тривалого, що відповідає принципам стратегічного управління підприємством. Таким чином, інформація повинна не тільки постійно обновлятися або модифікуватися, а й забезпечувати стабільність процесів, у яких вона використовується протягом часових циклів, тривалість яких визначається характером задач рівнів управління підприємством.

Отже, інформаційні продукти повинні задовольняти вимоги стабільності, що в запропонованому методі відповідає досить тривалим стадіям формування і становлення інформаційного продукту – для менеджерів нижчої й середньої ланок, і менш тривалим стадіями розвитку інформаційного продукту – для менеджерів вищої ланки. Таке припущення відповідає принципам побудови структури, системи управління і характеру прийнятих на підприємстві управлінських рішень, які наведені в табл. 4.

Таблиця 4

Етапи ЖЦ ІП на різних рівнях управління підприємством

Рівень управління	Характер управлінських рішень	Етап ЖЦ ІП
Вищий	Прийняття і затвердження (стратегічні рішення)	Розвиток
Середній	Прийняття до відома, розробка заходів (тактичні рішення)	Становлення, розвиток
Нижчий	Операційний менеджмент (оперативні рішення)	Формування, становлення

Найменш стійким етапом ЖЦ ІП є етап розвитку та його підетапи, тривалість яких визначається:

впливом зовнішнього середовища, що формує необхідність зміни стратегічних цілей або їхню адаптацію;

окремими властивостями інформації – підвищеною цінністю й корисністю інформаційного продукту;

формою та змістом інформаційного продукту.

Складність стану інформаційного продукту на стадії розвитку визначає собою його більшу нестабільність щодо стабільності на інших етапах ЖЦ ІП: характеризується більш високою алгоритмічною складністю (алгоритмів, методів і засобів перетворення інформації) та концептуальною складністю (методами, що використовуються для одержання інформації, механізмами перетворення інформації та її аналізу відповідно до стратегічних цілей підприємства).

Запропонований метод реалізує вирішення поставленої задачі на основі наступної послідовності етапів:

1) визначення складу виконавців, що відносяться до різних рівнів менеджменту підприємства (вищий, середній, нижчий);

2) визначення прав доступу до інформаційних продуктів персоналу, який відповідає цим рівням управління;

3) розкриття відповідно до посадових інструкцій персоналу функцій управління, які визначають виконання функцій забезпечення стабільності інформаційного продукту, включаючи такі процеси, як модифікація, верифікація, аудит;

4) визначення часових проміжків, що відповідають етапам ЖЦ ІП, протягом яких необхідна підтримка властивостей стабільності інформаційного продукту;

5) інтеграція засобів захисту властивостей інформації на різних рівнях управління підприємством в існуючу систему захисту інформації;

6) інтеграція локальних засобів захисту (мереж підприємства) у загальну корпоративну інформаційну систему підприємства.

Таким чином, пропонується наступне визначення стабільності ІС підприємства для забезпечення її інформаційної безпеки: *стабільність функціонування ІС підприємства визначається стабільністю всіх процесів, що відбуваються в інформаційній інфраструктурі підприємства у виробництві інформаційних продуктів і послуг протягом їхніх життєвих циклів, а також стабільністю функціонування окремих її елементіві та зв'язків між ними.*

Поняття стабільності системи нерозривно пов'язане з її стабільністю щодо внутрішніх і зовнішніх впливів, які можуть носити дестабілізуючий (деструктивний) характер. До таких дестабілізуючих впливів віднесемо ті, які відповідають різним етапам обробки інформації:

етап введення: введення перекручених даних, неавторизована модифікація введених даних, некоректна верифікація даних, що вводяться (відсутність процедур верифікації);

етап обробки: некоректні алгоритми, перепрограмування алгоритмів, програмних кодів, методів доступу до баз даних, обмеження доступу до баз даних;

етап аналізу результатів: некоректна інтерпретація, відсутність компетенції аналітиків, навмисне перекручування інформації, її використання для сумнівних угод, порушення прав доступу й т. п.

Забезпечення інформаційної безпеки *економічних суб'єктів передбачає усвідомлення змісту таких* понять, як "інформаційна зброя", "інформаційна війна", "інформаційна протидія" що, у свою чергу, показує їх зв'язок з наступними факторами:

інформаційно-комунікаційними – конвергенцією нових інформаційних технологій та їхнім впливом на різноманітні сфери діяльності і механізми функціонування суспільства [14; 15];

впливом масової культури на свідомість і поведінку людей за допомогою широкодоступних каналів передачі інформації;

стандартизацією способу життя більшості населення;

розвитком засобів маніпулювання людьми, тобто здійсненням на стан останніх таких регуляторних механізмів інформаційного впливу, які б дозволили протягом тривалого проміжку часу зберігати й підтримувати його для досягнення поставлених цілей [16].

Такі припущення можуть бути покладені в основу формування наступних визначень і понять.

Розглянемо процеси інформаційної взаємодії як процеси, що мають інформаційний характер і визначаються за допомогою:

змісту циркулюючої на підприємстві інформації;

ЖЦ ІП та її носіїв;

методів і засобів, що дозволяють створювати (відтворювати) всі види інформаційних потреб (товарів та послуг);

користувачів інформації різних рівнів управління;

життєвих циклів компонентів (елементів) інформаційної інфраструктури.

Результатом інформаційних взаємодій може бути одержання інформації з метою власного розвитку, з метою створення умов для розширення власного життєвого простору, а також навмисного (прямого) або ненавмисного впливу на цю інформацію з метою її перекручування та впливу на інформаційну інфраструктуру одного із суб'єктів інформаційної взаємодії (іншого об'єкта). Результат інформаційної взаємодії – інформаційна війна – це завдання збитків інформаційній інфраструктурі супротивника за рахунок порушення діяльності або функціонування окремих її підсистем (елементів) або зв'язків між ними [17; 18].

Засоби інформаційної війни – це такі засоби, які дозволяють здійснювати з інформацією, що передається, одержується або оброблюється, дії, які наносять збиток інформаційній інфраструктурі об'єкта з метою одержання переваги в інформаційному просторі – процесах виробництва й використання інформаційних продуктів і послуг, елементах інформаційної інфраструктури, процесах технології обробки, що відносяться до внутрішніх та зовнішніх інформаційних полів (складових інформаційного поля об'єкта).

Структура зовнішнього інформаційного поля визначається зовнішнім інформаційним образом підприємства, що містить у собі:

імідж, торговельну марку (бренд), репутацію;

канали доставки образу – ЗМІ, конференції, PR-акції;

інформаційні технології — технології, інновації, нововведення;

диференціацію продукції як засіб розширення свого життєвого простору;

конкурентоспроможність в області (сфері) його діяльності;

доступ до сучасних міжнародних інформаційних комунікацій.

Структура внутрішнього інформаційного поля визначається існуючою інформаційною інфраструктурою об'єкта.

Припущення про наявність внутрішнього і зовнішнього інформаційних полів дозволяє визначити інформаційну війну як цілеспрямований вплив інформаційних просторів суб'єктів взаємодії (інформаційних систем і інформаційних продуктів) на інформаційний простір об'єкта впливу з метою нанесення йому економічного збитку за рахунок дестабілізації функціонування внутрішнього та зовнішнього інформаційного полів.

Для конкретизації об'єктів, що беруть участь в інформаційній війні, введемо поняття "інформаційна мішень" – це та частина інформаційного простору, що у певний час піддається "атаці" з метою досягнення найбільшого ефекту/збитку.

Для розробки механізмів протидії інформаційним війнам визначимо *наступні принципи протидії засобам* їхнього ведення (інформаційній зброї):

1. Принцип системності.

2. Принцип постійного вдосконалення і підвищення рівня інформаційної безпеки підприємства.

3. Принцип контролю над всіма процесами, щодо яких визначений рівень конфіденційності і/або в яких здійснюється модифікація даних і доступ до них.

4. Принцип керованої та контрольованої зміни коду програмних засобів, що використовуються, реконфігурації компонент ІС (архітектури) відповідно до заданого алгоритму (принцип керованої адаптації архітектури ІС і реінжинірингу програмного забезпечення).

5. Принцип узгодження (координації) вбудованих механізмів протидії і захисту з існуючим організаційно-управлінським механізмом управління підприємством.

6. Принцип раціональності вибору заданого рівня інформаційної безпеки.

7. Принцип рефлексії, який полягає в постійній модифікації уразливих місць у ІС підприємства, відомих нападаючій стороні, яка веде інформаційну війну.

9. Принцип погодженості існуючої національної політики забезпечення інформаційної безпеки, чинної нормативно-правової бази, стандартів з політикою підприємства у сфері інформаційної безпеки.

10. Принцип відповідності механізмів забезпечення інформаційної безпеки організаційно-управлінському механізму забезпечення економічної безпеки підприємства.

Факторами, що впливають на організацію й протидію інформаційним війнам у різних формах їх ведення, є такі:

1. *Фактор часу*. Визначає оперативність і своєчасність вживання заходів із захисту підприємства від впливів, пов'язаних із проведенням інформаційних війн.

2. *Здатність захистити підприємство*. Характеризує існуючий рівень захищеності поточного стану підприємства з урахуванням захисту від усіх форм прояву інформаційної війни.

3. *Можливості атакуючої сторони.* Показує можливий рівень небезпеки для підприємства бути підданим інформаційним війнам з боку зовнішнього середовища.

4. *Величина ризику завдання збитків.* Ураховує загальний ризик піддатися впливу загроз і одержати збиток, який має певний характер (фатальний, помірний, слабкий).

На основі наведених факторів сформуємо структуру механізму прояву факторів, яка характеризує протидію інформаційним війнам і зведена в табл. 5.

Механізми протидії інформаційній зброї та інформаційним війнам повинні базуватися на посиленні позитивних факторів – інформаційної інфраструктури – і зменшенні (нейтралізації) негативних факторів, перепрограмуванні інформаційної інфраструктури на основі таких дестабілізуючих дій, як навмисна модифікація та інтерпретація інформаційних продуктів і їхніх похідних з метою виділення таких процедур, технологій маніпулювання ними, які дозволили б досягти переваги в матеріальній сфері.

Це завдання може бути вирішене за допомогою протидії і нейтралізації загроз інформаційних війн, які привели б до посилення "розтискаючої" сили внутрішніх та зовнішнього інформаційних полів (позитивних факторів) і зменшенню впливу "стискаючої" сили з боку інших суб'єктів інформаційної взаємодії (негативних факторів).

Таблиця 5

Структура механізмів прояву факторів

Прояв фактора	Елементи механізму прояву фактора
1. Оперативність і своєчасність вживання заходів із захисту підприємства від впливів, пов'язаних з веденням інформаційних війн	1.1. Своєчасна модифікація *(upgrade)* існуючих на підприємстві програмно-апаратних засобів для захисту від атак. 1.2. Адаптація контуру захисту підприємства відповідно до вимог міжнародного стандарту загальних критеріїв (ЗК) ISO/IEC 14508. 1.3. Використання сучасних технологій, що відповідають "духу" часу і характеру проведених інформаційних війн. 1.4. Своєчасне й безперервне навчання персоналу у сфері інформаційної безпеки. 1.5. Швидка адаптація до змінних форм інформаційних війн за рахунок упровадження новітніх технологій забезпечення захисту від атак
2. Рівень захищеності інформаційної системи з урахуванням усіх форм прояву інформаційної війни для поточного стану підприємства	2.1. Характеристика, рівень захищеності від атак усіх компонентів інформаційної інфраструктури. 2.2. Відповідність рівня захищеності компонент інформаційної інфраструктури різних рівнів управління підприємства вимогам конфіденційності інформації, які визначають рівні доступу до неї. 2.3. Рівень адаптивності (адаптивність) системи захисту підприємства щодо різних форм ведення інформаційної війни, включаючи програмне забезпечення, технічні засоби, засоби адміністрування, забезпечення винятково авторизованого доступу до інформації й т. д. 2.4. Наявність програм переходу на стандарти загальних критеріїв ISO/IEC 14508 з метою стандартизації й уніфікації засобів захисту. 2.5. Наявність компонентів організаційної структури для реалізації задач підвищення рівня захищеності підприємства (створення й розвиток служби інформаційної безпеки підприємства). 2.6. Підвищення психологічної стабільності персоналу підприємства і підтримка його на належному рівні для створення відповідного соціально-психологічного клімату
3. Рівень небезпеки для підприємства бути підданим інформаційним війнам з боку зовнішнього середовища	3.1. Рівень схильності атакам з боку зовнішнього середовища на основі аналізу положення і конкурентоспроможність його в галузі, конкурентоспроможність галузі в цілому у сформованих ринкових умовах (зовнішнє середовище). 3.2. Визначення найбільш уразливих місць, які можуть бути піддані атакам різних форм і змісту (рефлексивний підхід). 3.3. Визначення рівня соціальної напруженості в регіоні, на підприємстві (соціальний фактор). 3.4. Наявність потенційних шкідників на самому підприємстві, які використовують методи ведення інформаційної війни (розвідники, диверсанти)
4. Величина ризику одержати збиток, що має певний рівень (фатальний, помірний, слабкий)	4.1. Зміст, характеристика збитку (матеріального, фінансового). 4.2. Визначення кількісних і якісних характеристик збитку. 4.3. Вибір критеріїв і правил для визначення ризиків. 4.4. Моделювання характеристик збитку від впливу інформаційних війн на основі моделей "порушника" і визначення найбільш несприятливих (сприятливих) сценаріїв розвитку подій у процесі організації системи захисту з метою мінімізації ризиків

Протидії можуть носити пасивний (нейтралізуючий) і активний характери.

Пасивні протидії можуть містити в собі вирішення наступних завдань:

1. Кількісна і/або якісна оцінка поточного та необхідного рівня інформаційної безпеки при заданих рівнях конфіденційності інформації для різних рівнів управління підприємством.

2. Розробка заходів щодо реінжинірингу системи безпеки ІС для досягнення її заданого рівня.

3. Проведення аудиту і сертифікації компонентів інформаційної системи в цілому на відповідність вимогам та існуючим стандартам інформаційної безпеки.

4. Розробка зон відповідальності для взаємодії служб і підрозділів зі службою інформаційної безпеки підприємства. Розробка організаційно-розпорядницької документації з координації й реалізації заходів щодо забезпечення необхідного рівня захисту із припустимими рівнями ризиків.

5. Розробка політики і концепції забезпечення інформаційної безпеки підприємства на період 3 – 5 років із визначенням осіб, відповідальних за її реалізацію.

Активні протидії становлять сукупність методів, засобів, правил здійснення впливу на інформаційні простори (інформаційні інфраструктури) суб'єктів взаємодії з метою запобігання і нейтралі-

зації інформаційних атак та вироблення власної політики в інформаційній сфері для забезпечення стабільного розвитку підприємства.

До основних завдань у забезпеченні активної протидії відносяться наступні:

1. Збільшення "своїх" засобів і каналів інформаційного впливу на суспільну думку (захоплення, перехоплення й постановка під свій вплив різних ЗМІ).

2. Протидія і розробка цільових заходів з недопущення витоку інформації.

3. Підвищення іміджу й репутації підприємства за рахунок публікації достовірної та об'єктивної інформації про підприємство в урядових, регіональних ЗМІ, що мають високий рівень репутації.

4. Постійна сертифікація наявного та придбаного ліцензійного устаткування, рівень інформаційної безпеки якого гарантується, що дозволить забезпечити імідж підприємства як такого, що має високий рівень захищеності.

5. Широке використання засобів контррозвідувальної діяльності з метою визначення місцезнаходження підслуховуючих пристроїв, засобів радіоелектронної війни, комп'ютерної хакерської діяльності.

6. Постійний контроль точок входу зовнішніх комунікаційних систем в інформаційну систему підприємства, особливо в корпоративних системах, що використовують віддалені комп'ютерні термінали, з метою виявлення спрямованого інформаційного впливу для порушення їхньої діяльності.

Формування підприємством механізмів, сполучених з механізмами прояву факторів інформаційної безпеки і безпеки ресурсів підприємства в цілому, дозволить сформувати стійкі режими функціонування ІС і підвищити якість керованого розвитку підприємства.

Література: 1. Андрощук Г. А. Экономическая безопасность предприятия: защита комерческой тайны: Монография / Г. А. Андрощук, П. П. Крайнев. – К.: Изд. дом "Ин Юре", 2000. – 400 с. 2. Козаченко Г. Б. Економічна безпека підприємства: сутність та механізм забезпечення: Монографія / Г. Б. Козаченко, В. П. Пономарьов, О. М. Ляшенко. – К.: Лібра, 2003. – 280 с. 3. Олейников Е. А. Основы экономической безопасности (государства, регион, предприятие, личность) / Под ред. Е. А. Олейникова. – М.: ЗАО "Бизнес-школа "Интелект-Синтез", 1997. – 288 с. 4. Тамбовцев В. Л. Экономическая безопасность хозяйственных систем: Структура проблемы // Вестник Московского гос. унив. Сер. "Экономика". – 1995. – №3. – С. 3 – 9. 5. Шлыков В. В. Комплексное обеспечение экономической безопасности предприятия. – СПб.: ЗАО "Информационное агентство "Кредит-реформа – Санкт-Петербург", 1999. – 138 с. 6. Пономаренко В. С. Экономическая безопасность региона: анализ, оценка, прогнозирование: Монография / В. С. Пономаренко, Т. С. Клебанова, Н. Л. Чернова. – Харьков: ИД "ИНЖЭК", 2004. – 144 с. 7. Прохожев А. А. Национальная безопасность. основы теории, сущность, проблемы. – М.: РАГС, 1997. – 28 с. 8. Куркин Н. В. Метод повышения устойчивости и обеспечения безопасности информационных систем предприятия // Економіка промисловості: – 2003. – №2(20). – С. 105 – 109. 9. Пярин В. А. Безопасность электронного бизнеса / В. А. Пярин, А. С. Кузьмин, С. Н. Смирнов. – М.: Гелиос-АРВ, 2002. – 432 с. 10. Терминологические основы проблематики информационной безопасности. Материалы к заседанию Межведомственного междисциплинарного семинара по научным проблемам информационной безопасности 1 марта 2001 г. МГУ, кафедра информационной безопасности. – М.: Изд. МГУ, 2001. – 20 с. 11. Устинов Г. Н. Основы информационной безопасности систем и сетей передачи данных. – М.: СИНТЕГ, 2000. – 248 с. 12. Концепція (основи державної політики) національної безпеки України, схвалена Верховною Радою України 16 січня 1997 року. // www.nbuv.gov.ua. 13. Соколов А. В. Как оценить угрозы безопасности информации? // Элвис + / http://www.elvisplus.ru. 14. Пономаренко В. С. Стратегічне управління підприємством. – Харків: Основа, 1999. – 620 с. 15. Приходько А. Я. Информационная безопасность в событиях и фактах. – М.: СИНТЕГ, 2001. – 260 с. 16. Гаврюшин Е. Человеческий фактор в обеспечении безопасности конфиденциальной информации // В мире права. – 2002. – №2. – С. 29 – 32. 17. Гаврюшин Е. Человеческий фактор в обеспечении безопасности конфиденциальной информации // В мире права. – 2002. – №2. – С. 29 – 32. 18. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: Минобразования россии, 1997. – 536 с. 19. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, Л. М. Ивашенко. – М.: Горячая линия – Телеком, 2000. – 452 с. 20. Путятин Ю. А. Финансовые механизмы стратегического управления развитием предприятия / Ю. А. Путятин, А. И. Пушкарь, А. Н. Тридед. – Харьков: Основа, 1999. – 488 с. 21. Шурухнов Н. Г. Расследование неправомерного доступа к компьютерной информации. – М.: Щит-М, 1999. – 256 с.

Зміст

Секція 1
Методи та технології безпеки інформаційних систем

Секція 2
Захист інформації в комп'ютерних системах

Секція 3
Інформаційні та телекомунікаційні системи в бізнесі

Довідка про авторів

Альбощій О. В. – канд. воєн. наук, доцент Університету цивільного захисту України

Попов В. М. – канд. техн. наук, проректор по роботі з персоналом Університету цивільного захисту України

Акімов В. В. – докт. сільгосп. наук, професор Харківського національного університету внутрішніх справ

Назаренко Д. В. – викладач ХНЕУ

Кобзев І. В. – канд. техн. наук, доцент Харківського національного університету внутрішніх справ

Калякін С. В. – викладач Харківського національного університету внутрішніх справ

Горелов Ю. П. – канд. техн. наук, доцент Харківського національного університету внутрішніх справ

Задачин В. М. – канд. фіз.-мат. наук, доцент ХНЕУ

Павленко Л. А. – канд. техн. наук, доцент ХНЕУ

Грищук Р. В. – канд. техн. наук, науковий співробітник Житомирського військового інституту ім. С. П. Корольова Національного авіаційного університету

Живко М. О. – ад'юнкт ЛьвДУВС

Босак Х. З. – курсант ЛьвДУВС

Заєць В. В. – аспірант НАУ

Чуприн В. М. – канд. техн. наук, професор НАУ

Ревак І. О. – канд. екон. наук, доцент Львівського державного університету внутрішніх справ

Дудикевич В. Б. – докт. техн. наук, професор Національного університету "Львівська політехніка"

Максимович В. М. – канд. техн. наук, доцент Національного університету "Львівська політехніка"

Кавун С. В. – канд. техн. наук, доцент ХНЭУ

Сорбат И. В. – преподаватель ХНЭУ

Колесников А. Н. – канд. техн. наук, доцент Харьковского филиала Украинского государственного центра радиочастот

Колесников С. А. – студент ХНУРЭ

Кобозева А. А. – канд. физ.-мат. наук, доцент Одесского национального политехнического университета

Безмалый В. Ф. – руководитель программы подготовки администраторов информационной безопасности ООО "БМС Консалтинг" (г. Киев)

Кузнецов А. А. – докт. техн. наук, ст. научный сотрудник Харьковского университета Воздушных Сил им. Ивана Кожедуба

Король О. Г. – преподаватель ХНЭУ

Ткачов А. М. – канд. техн. наук, научный сотрудник Харьковского университета Воздушных Сил им. Ивана Кожедуба

Купрейчик И. В. – канд. техн. наук, доцент ХНЭУ

Евсеев С. П. – канд. техн. наук, доцент ХНЭУ

Чевардин В. Е. – канд. техн. наук, доцент Военного института телекоммуникаций и информатизации НТУУ "КПИ"

Радковский С. А. – канд. техн. наук, доцент Донецкого института железнодорожного транспорта

Харьбин А. В. – канд. техн. наук, доцент Военного института телекоммуникации и информатизации НТУУ "КПИ"

Сорокин И. А. – начальник отделения ВТ учебной лаборатории кафедры Военного института телекоммуникации и информатизации НТУУ "КПИ"

Гросфельд Ю. А. – ст. преподаватель Запорожского национального технического университета

Костів Ю. М. – аспірант Національного університету "Львівська політехніка"

Шарапов В. Г. – аспірант Військового інституту телекомунікацій та інформатизації НТУУ "КПІ"

Васильєва А. А. – студент Запорізького національного технічного університету

Горбань В. Б. – головний спеціаліст сектору фінансового аналізу відділу комунальних підприємств Управління економіки Департаменту економічної політики Львівської міської ради

Беседовський О. М. – канд. екон. наук, доцент ХНЕУ

Гаврилова А. А. – викладач ХНЕУ

Khodyrevskaya A. V. – trainee KhNEU

Хома В. В. – докт. техн. наук, професор Національного університету "Львівська політехніка"

Гарасим Ю. Р. – студент Національного університету "Львівська політехніка"

Живко З. Б. – канд. екон. наук, доцент, професор Львівського державного університету внутрішніх справ

Войтович Ю. В. – студент ЛьвДУВС

Кузнецова С. А. – канд. екон. наук, доцент, докторант Державного вищого навчального закладу "Київський національний економічний університет ім. Вадима Гетьмана"

Жукарєв В. Ю. – викладач ХНЕУ

Огурцов В. В. – канд. екон. наук, доцент ХНЕУ

Пономарьова К. В. – викладач ХНЕУ

Пашковський В. В. – канд. техн. наук, ст. науковий співробітник Інституту Сухопутних військ ім. Петра Сагайдачного Національного університету "Львівська політехніка"

Podbregar I. – prof. Ph.D., Faculty of Criminal Justice and Security, Kotnikova 8, 1000 Ljubljana

Brumnik R. – Ph.D. candidate, Metra engineering d.o.o., Quality manager, Faculty of Criminal Justice and Security

Куркін М. В. – докт. екон. наук, професор

Комарова А. Б. – студент Запорожского национального техничного университета

Мисюра А. А. – канд. физ.-мат. наук, доцент Запорожского национального техничного университета

Поляков А. А. – канд. техн. наук, преподаватель ХНЭУ

Жученко А. С. – канд. техн. наук, доцент Украинской государственной академии железнодорожного транспорта

Лысечко В. П. – канд. техн. наук, доцент Украинской государственной академии железнодорожного транспорта

Бурдаев В. П. – канд. физ.-мат. наук, доцент ХНЭУ

Баранник В. В. – докт. техн. наук, ведущий научный сотрудник Харьковского университета Воздушных Сил им. Ивана Кожедуба

Хаханова А. В. – аспирант ХНУРЭ

Голубев В. А. – канд. юр. наук, доцент Донецкого юридического института Луганского государственного университета внутренних дел

Калашников А. А. – канд. техн. наук, преподаватель Университета гражданской защиты Украины

Лукацкий А. В. – бизнес-консультант по безопасности Cisco Systems в России и СНГ, консультант Cisco по информационной безопасности

Хомич В. М. – канд. юр. наук, профессор Белорусского государственного университета

Ходасевич А. А. – магистр права Белорусского государственного университета

Гринев Д. В. – ст. научный сотрудник Харьковского университета Воздушных Сил им. Ивана Кожедуба

Паржин Ю. В. – канд. техн. наук, ст. научный сотрудник, заместитель директора по учебной работе НИПО при НТУ "ХПИ"