УДК 004.738.5:338.46(075)

І.М. Пістунов, д-р техн. наук, проф.

Державний вищий навчальний заклад „Національний гірничий університет“, м.Дніпропетровськ, Україна,
e-mail: pistunovi @gmail.com

ВИЗНАЧЕННЯ РІВНЯ БЕЗПЕКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

I.M. Pistunov, Dr. Sci. (Tech.), Prof.

State Higher Educational Institution “National Mining University”, Dnipropetrovsk, Ukraine, e-mail: pistunovi@gmail.com

DETERMINATION OF THE E-COMMERCE SECURITY LEVEL

Мета. Компенсація ризику при діяльності комерційної установи, що працює в режимі електронної комерції, у напрямі його зменшення, визначення основних напрямів серед неорганізаційних заходів.

Методика. Застосовані методи теорії ймовірностей, математичної статистики та актуарних розрахунків.

Результати. Показано, що статистика запитів до інформаційної системи, яка обслуговує електронну комерцію підприємства, а також статистика втрат від дій інших осіб для підприємств, що працюють у цій галузі, дозволяє зменшити ризик. Визначені такі основні напрями зменшення ризиків в електронній комерції як визначення моменту початку кібератаки та страхування електронної комерції. Застосувавши методи теорії ймовірності у припущенні, що кількість запитів до інформаційної системи підлягає експоненційному закону розподілу, вдалося розрахувати, що, при перевищення на 50% кількості запитів, імовірність того, що почалася кібератака становить 0,9. Із застосуванням методів, залучених із актуарних розрахунків, у припущенні, що цей тип страхування відноситься до ризикового, була визначена величина нетто-ставки при страхуванні ризиків електронної комерції шляхом статистичних досліджень ринку.

Наукова новизна. Розрахунок критичної величини запитів на сайт для визначення початку кібератаки є оригінальною розробкою та має наукову новизну. Оригінальною також є методика визначення нетто-ставки при страхуванні електронної комерції.

Практична значимість. Усі положення статті готові для негайного використання в роботі структур, що займаються безпекою електронної комерції.

Ключові слова: *безпека, електронна комерція, кібератака, страхування*

Постановка проблеми. Інтернет-комерція, торгівля в Інтернеті – це комерційна діяльність в Інтернеті, коли процес покупки / продажу товарів або послуг (весь цикл комерційної / фінансової транзакції або її частина) здійснюється електронним чином із застосуванням Інтернет-технологій. Електронна комерція (e-commerce): маркетинг, подача пропозицій, продаж, здача в оренду, надання ліцензій, постачання товарів, послуг або інформації з використанням комп’ютерних мереж або Інтернету.

Економічною передумовою електронної комерції є об’єктивна необхідність зниження витрат, що виникають у комерційних циклах. Технічною передумовою електронної комерції став стрімкий розвиток служб Інтернету.

Для покупця однією з головних переваг електронної комерції є значна економія часу на отримання інформації про товар, його вибір.

Усі розрахунки в електронній комерції здійснюються через Інтернет-банкінг – забезпечення клієнту можливості управління банківським рахунком через Інтернет на основі систем електронних платежів. Окрім цього, управління банківськими рахунками через Інтернет складає основу систем дистанційної роботи на ринку цінних паперів та віддаленого страхування.

Водночас зі зростанням кількості послуг зростає й небезпека, оскільки значна кількість чинників може викликати втрати та збитки при проведенні електронних операцій.

З урахуванням сформованої практики забезпечення інформаційної безпеки виділяють такі напрями захисту інформації [1]. Їх перелік наступний:

1. Правовий захист – спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі.

2. Організаційний захист – регламентація діяльності та взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією і явище внутрішніх і зовнішніх загроз.

3. Інженерно-технічний захист – сукупність спеціальних органів, технічних засобів і заходів щодо їх використання в інтересах захисту конфіденційної інформації.

Аналіз останніх досліджень. Загрози, пов'язані з діями, які люди вчиняють, розділяються на ненавмисні та навмисні [2].

Автором досліджено, що ненавмисні дії люди вчиняють випадково, через незнання, неуважність або недбалість, з цікавості, але без злого наміру:

- ненавмисні дії, що призводять до часткової або повної відмови системи, руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисне псування устаткування, видалення, перекручування файлів з важливою інформацією або програм, у тому числі системних і т.п.);

© Пістунов І.М., 2015

- неправомірне відключення устаткування або зміна режимів роботи пристроїв та програм;

- ненавмисне псування носіїв інформації;

- запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або здійснювати незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.п.);

- нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін., що не є необхідними для виконання порушником своїх службових обов'язків) з подальшим необґрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті та пам'яті на зовнішніх носіях);

- зараження комп'ютера вірусами;

- необережні дії, що призводять до розголошення конфіденційної інформації або роблять її загальнодоступною;

- розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів, шифрування, ідентифікаційних карток, перепусток і т.п.);

- проектування архітектури системи, технології обробки даних, розробка прикладних програм з можливостями, що несуть небезпеку для працездатності системи та безпеки інформації;

- ігнорування організаційних обмежень при роботі в системі;

- вхід до системи в обхід засобів захисту (завантаження сторонньої операційної системи з дискети й т.п.);

- некомпетентне використання, налаштування або неправомірне відключення засобів захисту персоналом служби безпеки;

- пересилання даних за хибною адресою абонента (пристрою);

- уведення помилкових даних;

- ненавмисне пошкодження каналів зв'язку.

Навмисні загрози автором визначаються наступним чином. Ці дії людей здійснюються навмисне для дезорганізації роботи системи, виведення системи з ладу, проникнення до системи та несанкціонованого доступу до інформації:

- фізичне руйнування системи (шляхом вибуху, підпалу тощо), вивід з ладу всіх або окремих найбільш важливих компонентів АС (пристроїв, носіїв важливої системної інформації, осіб із числа персоналу й т.п.);

- відключення або вивід з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);

- дії з дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи й т.п.);

- впровадження агентів в число персоналу системи (у тому числі, можливо, і в адміністративну групу, яка відповідала за безпеку);

- вербовка (шляхом підкупу, шантажу й т.п.) персоналу чи окремих користувачів, що мають певні повноваження;

- застосування пристроїв для підслуховування, дистанційної фото- та відеозйомки й т.п.;

- перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і каналів зв'язку, а також наводок активних випромінювань на допоміжні технічні засоби, що безпосередньо не беруть участі в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

- перехоплення даних, переданих по каналах зв'язку, та їх аналіз з метою з'ясування протоколів обміну, правил входження у зв'язок і авторизації користувача, подальших спроб їх систематизації для проникнення до системи;

- розкрадання носіїв інформації (магнітних дисків, стрічок, запам'ятовуючих пристроїв і самих персональних комп'ютерів);

- несанкціоноване копіювання носіїв інформації;

- розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації й т.п.);

- читання залишкової інформації з оперативної пам'яті та зовнішніх запам'ятовуючих пристроїв;

- читання інформації з областей оперативної пам'яті, використовуваних операційною системою (у тому числі підсистемою захисту) або іншими користувачами, в асинхронному режимі, використовуючи недоліки мультизадачних операційних систем і систем програмування;

- незаконне одержання паролів та інших реквізитів доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи й т.д.) з наступним маскуванням під зареєстрованого користувача;

- несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як: номер робочої станції в мережі, фізичну адресу, адреси в системі зв'язку, апаратний блок кодування й т.п.;

- злам шифрів криптозахисту інформації;

- впровадження апаратних, програмних „закладок" і „вірусів" („троянських коней" і „жучків"), тобто таких ділянок програм, що не потрібні для здійснення заявлених функцій, але дозволяють долати систему захисту, потай і незаконно здійснювати доступ до системних ресурсів з метою реєстрації та передачі критичної інформації, дезорганізації функціонування системи;

- незаконне підключення до ліній зв'язку з метою роботи „між рядків", з використанням пауз у діях законного користувача від його імені з наступним уведенням помилкових спілкувань або модифікацією переданих повідомлень;

- незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу до системи та успішної аутентифікації з подальшим уведенням дезінформації чи нав'язуванням хибних повідомлень.

Виділення невирішених раніше частин загальної проблеми. Вирішення задачі убезпечити електронну комерцію від дії людей викликає низку органі-

заційних заході [3–6]. Розглянемо деякі з них в авторському викладені.

Для того, щоб виявити зловмисні дії людей, потрібне:

• гарне програмне забезпечення поточного контролю;

• регулярна перевірка системних журналів;

• система стеження.

Припустивши, що програмне забезпечення знаходиться в порядку, найбільш очевидні сліди злочину можуть бути розділені на дві категорії: зовнішні та внутрішні. Зовнішніми слідами, пов'язаними зі спробами впровадження в комунікаційну лінію зв'язку, є:

- виведені з ладу сигнальні пристрої на кабелях зв'язку;

- посилення загасання сигналів в оптичній лінії зв'язку;

- зміни в напрузі, ємності, опорі або частоті.

Внутрішніми слідами, пов'язаними зі спробою отримати доступ через звичайний вхідний набір або з дистанційного тракту, є:

- телефонні дзвінки різної тривалості в кімнату, коли після відповіді можна почути звуки модему, що вказують на атаку, проведену шляхом послідовного автоматичного набору диска;

- повторювані безуспішно спроби входу в систему;

- повторювання передач керуючих команд;

- часте використання підказок;

- нерозв'язана або незапланована робота;

- образливі або наклепницькі повідомлення;

- знищена або зіпсована інформація;

- переміщені або змінені файли та новостворені довідники;

- скарги замовників, постачальників і користувачів на виникаючі час від часу помилки й труднощі входу та роботи в системі.

Організація повинна постаратися хоч б на один крок випередити хакера. Інформація про особу злочинця може бути зібрана, наприклад, за допомогою:

- звернення до місцевого провайдера, щоб перевірити наявність облікової інформації щодо державної структури в секції зловмисника;

- підтримання зв'язку з відділом кадрів, що займається проблемами незадоволених або чимось занепокоєних службовців;

- використання інших хакерів в якості інформаторів без ознайомлення їх з деталями системи даної фірми, наприклад, через третіх осіб.

Щоб виявити потенційну активність промислового шпигуна або професійного хакера, організація повинна освоїти різні методи:

- виявити спроби крадіжки можна, наприклад, прихованою камерою, спрямованою на мішки з роздруківками, приготованими до вивозу;

- перевірити добромисність усіх відвідувачів, зокрема фахівців із засобів зв'язку, електриків, водопровідників, а також торгових агентів.

Особливо небезпечними місцями є приміщення, де окрім державних установ, існують орендовані декількома фірмами приміщення, в яких протягом дня можна побачити 10–15 фахівців різного роду, які прагнуть отримати доступ до головного вузла зв'язку. При цьому ідентифікаційні картки, що засвідчують особистість, перевіряються вкрай рідко. Відомо, що, використовуючи коридори та переходи в будівлях, співробітники проводять до приміщення сторонніх осіб. Від них слід вимагати пред'явлення стандартної ідентифікаційної картки з фотографією та документа, що показує, якого роду роботу виконує дана особа. Завжди слід звіряти по телефону ситуацію, коли заздалегідь підготовлений шифр або код отримав відмову повідомлення. Від службовця необхідно вимагати, щоби він фіксував шифр входу до головного вузла зв'язку, відзначаючи в журналі:

- дату та час відвідин;

- прізвище, ім'я;

- назву організації, для якої виконується робота;

- факт перевірки ідентифікаційної картки.

Реєстраційний журнал повинен періодично перевірятися. Усі відвідувачі мають бути ідентифіковані. Якщо прийшов відвідувач, він повинен пред'явити посвідчення своєї фірми та номер телефону, за яким безпосередньо можна навести довідки. Штат повинен бути попереджений про те, яких відвідувачів варто остерігатися.

Підозрілими можуть бути:

- сторонні особи, які стверджують, що вони шукають у даному будинку людини або фірму, якої немає в переліку установ, що орендують дане приміщення;

- потенційні відвідувачі, охочі в деталях дізнатися про цю установу, але, разом з тим, згадавши про мету свого візиту, намагаються не вдаватися в деталі щодо їх організації.

Штат секретарів, зазвичай, погано навчений тому, як розпізнати та які вжити дії проти енергійного, наполегливого відвідувача, який не бажає йти без інформації, за якою він прийшов. У подібних випадках секретарю потрібно проявити твердість і випровадити відвідувача або викликати помічників. Однак, частіше за все, у цих випадках інформація видається секретарем раніше, ніж виникає підозра. Щоб запобігти витоку секретної інформації повинна здійснюватися політика „чистих столів": ніякі документи не повинні залишатися на столах після закінчення робочого часу, усі непотрібні папірці повинні бути розірвані перед викиданням їх до корзини. Система реагування повинна бути влаштована таким чином, щоб всі скарги, що надійшли від відвідувачів, прохачів і користувачів, зіставлялися та аналізувалися. У цьому повинні допомогти пакети статистичного аналізу, що контролюють такі незвичайні явища, як:

- кожен вечір в один і той же час системи починають давати збій;

- з'являються помилкові повідомлення, спостерігаються помилки при передачі;

- спостерігається розбіжність результатів.

Як тільки виникають підозри щодо можливих розвідувальних дій або злочинів, потрібно розпочати повномасштабне розслідування. Велике число злочинів можна попередити, якщо слідувати основним правилам:

- організація не повинна публікувати телефонні номери комутованих портів і зобов'язана мати адресу колишнього директора в системі комутації;

- після встановлення зв'язку й до моменту входу користувача до системи, остання не повинна видавати ніякої інформації;

- у системі необхідно використовувати паролі, що складаються не менше, ніж із семи знаків, і коди користувачів повинні відрізнятися від запропонованих фірмою-виробником;

- повинна бути реалізована програма динамічних паролів для гарантії їх постійної зміни при звільненні службовців з даної установи;

- функції терміналів повинні бути точно визначені, наприклад, платіжні відомості повинні вводитися тільки через певні термінали.

Щоб перешкодити злочинцям отримати несанкціонований доступ, необхідно технологію захисту пов'язати з технологічними процесами організації. Повинна бути проведена оцінка ризику з тим, щоб витрати на засоби управління й контролю відповідали ступеню ризику. Організація повинна шукати засоби для зниження мотивації злочинів шляхом запровадження:

- паролів і процедур персональної ідентифікації;
- засобів контролю за операційною системою;
- контролю доступу;
- контролю за базою даних;
- контролю за мережею.

Простий перегляд усіх необхідних заходів безпеки показує, що, окрім декларативних рекомендацій, не існує конкретних цифрових методів визначення зловмисних дій людей.

Постановка завдання. Визначити найбільш вразливі напрями роботи електронної комерції та розробити методику їх числового визначення.

Виклад основного матеріалу дослідження. Статистичні спостереження за роботою власної інформаційної системи підприємства та за роботою аналогічних підприємств дозволить, у значні мірі, убезпечити роботу підприємства, що діє в режимі електронної комерції. Покажемо це на двох, найбільш популярних напрямах захисту електронного бізнесу.

Серед одних із найбільш відомих явищ кіберзлочинності є спроби припинити діяльність комерційного підприємства через Інтернет. Одну з найбільших загроз діяльності підприємства, що діє в режимі електронної комерції, представляє кібератака. Цей тип зумисних дій можна вважати такими, що легко виявляється та діагностується.

Інші типи загроз електронній комерції діагностувати значно складніше, тому найкращим виходом із ситуації буде страхування бізнесу. У цьому випадку комерційній структурі не варто покладатися на розрахунки, зроблені страховою компанією, а самостійно визначити нетто-ставку, щоб зменшити надмірні страхові виплати.

Розрахунок початку кібератаки. Кібератакою називається ситуація, коли кількість звернень з Інтернету до інформаційної системи (ІС), що обслуговує запити клієнтів через Інтернет, різко зростає [1]. При цьому, сервер ІС починає працювати все повільніше, намагаючись задовольнити всі запити, доки не припиняє роботу через перевантаження.

Визначити початковий момент кібератаки дуже важливо, оскільки це дозволить зменшити втрати на компенсацію її наслідків, шляхом вимкнення ІС або визначення IP-адреси, звідки надходить спам, з наступним блокуванням цього напряму надходження повідомлень.

Знайдемо критерій початку кібератаки за статистичними розрахунками. Для цього розіб'ємо весь період роботи інформаційної системи, що обслуговує зовнішні запити електронної комерції, на рівні проміжки часу. Ними можуть бути: година, доба, тиждень, але, в умовах роботи через Інтернет, краще встановити ці проміжки не більше ΔT = 20–30хв.

Далі потрібно налагодити постійний контроль за кількістю вхідних запитів. Після визначення кількості запитів у кожному проміжку не менше 40, потрібно розрахувати середню кількість звернень M_x.

Висунемо гіпотезу, що потік подій характеризується експоненційним законом розподілу. Він описується функцією розподілу виду [7]

$$F(x)=\int_0^x \lambda\cdot e^{-\lambda x}dx=1-e^{-\lambda x},\ \text{при } x\ge 0;$$
$$F(x)=0,\qquad\qquad \text{при } x<0.$$

Математичне сподівання експоненційного закону розподілу дорівнює

$$M_x=\int_0^\infty \lambda x e^{-\lambda x}dx=\frac{1}{\lambda}. \qquad (1)$$

Медіана може бути знайдена як

$$M_e=-\mathrm{Ln}0{,}5/\lambda\approx 0{,}69/\lambda.$$

Звідки

$$\begin{cases}\lambda=\dfrac{1}{\mathrm{M_x}}\\ \lambda=-\dfrac{Ln0{,}5}{Me}\end{cases}. \qquad (2)$$

Вираз (3) дозволяє знайти зв'язок між медіаною та середнім

$$Me=-\frac{M_x}{Ln0.5}. \qquad (3)$$

Задамо довірчу ймовірність β, що визначить допустимий рівень імовірності попадання кількості вхідних звернень в інтервал $[Me; K]$, де K – реальне число звернень на проміжку ΔT. Очевидно, що ймовірність попадання на цей інтервал має складати половину довірчої ймовірності

$$\frac{\beta}{2}\ge P(\mathrm{Me<x<K})=\mathrm{EXP}(-\lambda\mathrm{Me})-\mathrm{EXP}(-\lambda\mathrm{K}). \qquad (4)$$

Підставимо значення λ із (2) у (4)

$$\frac{\beta}{2} \text{ з } EXP(-\frac{Me}{M_x}) - EXP(-\frac{K}{M_x}) \cdot$$

А медіану, у свою чергу, виразимо через середнє

$$\frac{\beta}{2} \text{ з } EXP(\frac{M_ч}{M_x Ln0.5}) - EXP(-\frac{K}{M_x}) \cdot$$

Приведемо вираз до виду

$$\beta \text{ з } 2 \times EXP(\frac{1}{Ln0.5}) - EXP(-\frac{K}{M_x}) =$$

$$= 0,47258018 - 2 \times EXP(-\frac{K}{M_x}).$$

Знайдемо тепер допустиме перевищення кількості вхідних викликів інформаційної системи над середнім їх значенням

$$\frac{\beta - 0,47258018}{2} \text{ з } -EXP(-\frac{K}{M_x}),$$

звідкіля

$$M_x \times Ln\left(\frac{\beta - 0,47258018}{2}\right) \text{з} K. \qquad (5)$$

Отже, якщо K (кількість звертань до ІС) перевищить значення виразу з лівої частини (5), можна вважати, що кібератака вже почалася.

Розуміючи, що вираз $\frac{K}{M}$ є перевищенням середнього у відносних одиницях, зробимо розрахунок відповідності деяких популярних значень довірчої ймовірності мірі перевищення кількості вхідних викликів над середнім. Результати розрахунків представлені в таблиці.

Таблиця

Розрахунок відповідності значення довірчої ймовірності та міри перевищення кількості вхідних викликів їх середнім значенням

β	$\frac{K}{M_x}$
0,6	2,753415
0,75	1,975370
0,8	1,809659
0,85	1,667544
0,9	1,543136
0,95	1,432506
0,98	1,371564
0,99	1,352048
0,999	1,334803
0,9999	1,333095

З таблиці можна зробити висновок, що, у разі перевищення кількості запитів до ІС над середньою їх кількістю тільки в півтора рази, можна з імовірністю більше 0,9 вважати, що кібератака вже почалася.

Обчислення нетто-ставки при страхуванні електронної комерції. При зверненні до страхових компаній бізнесмени, які працюють у галузі електронної комерції, можуть отримати значно завищену пропозицію за тарифними ставками або навіть відмову. Причиною цього є відсутність надійної статистики щодо можливих втрат при проведенні подібних операцій. Більше того, страховики просто не готові укладати такі договори через відсутність надійної страхової статистики. Тому перед укладанням договору страхування фірмам, що працюють у галузі електронної комерції, бажано самостійно провести дослідження щодо кількості випадків (n) втрати бізнесу через кіберзлочинність. Наступними показниками статистики будуть: N – загальна кількість організацій, що працюють у сфері електронної комерції; b – збиток від кіберзлочинності (ступінь знищення бізнесу); B – загальна сума договорів, що виконуються цими організаціями в рамках електронного бізнесу.

За цими даними визначимо середнє (M_b) та середнє квадратичне відхилення (σ_b) для збитку від кіберзлочинності.

Далі знаходиться коефіцієнт варіації

$$Var_b = \frac{\sigma_b}{M_b}.$$

Для розрахунку тарифної нетто-ставки необхідно використати довірчу ймовірність (β) та зворотне значення функції Лапласа $\Phi(\beta)$, наприклад, із застосуванням функції НОРМСТОБР електронних таблиць Excel.

Тоді тарифна нетто-ставка при страхуванні електронної комерції буде знайдена як [8]

$$T_n = \frac{n}{N}(1 + \Phi(\beta) \cdot Var_b).$$

Для прикладу, визначимо розмір нетто-ставки при страхуванні від кіберзлочинності, якщо кількість негативних випадків n = 13 при загальній кількості організацій, що працюють у галузі електронної комерції, становить N = 12456. Зворотне значення функції Лапласа $\Phi(\beta)$ =1,68 (для β = 0,95), середнє значення ступеня знищення об'єкта дорівнює M_b =1235478 грн при математичному стандарті σ_b =1235 грн.

Відповідно до формули (1), величина тарифної нетто-ставки складе

$$T_n = \frac{13}{12456}\left(1 + 1,68\frac{1235}{12345478}\right) = 0,0010819.$$

Результат розрахунку дозволяє сказати, що при страхуванні бізнесу на суму 1млн грн нетто-ставка складе 1081,9 грн.

Треба враховувати, що страхові компанії до нетто-ставки додають навантаження, що в декілька разів перевищує саму нетто-ставку. Але в усіх випадках, якщо запропонований страховий брутто-тариф буде перевищувати нетто-ставку більше, ніж на порядок, варто ознайомити менеджерів страхової компанії з цими розрахунками для зменшення брутто-тарифу або відмовитися від таких страхових послуг і пошукати іншого страховика.

Висновки. Проведені дослідження показали, що:

1. За статистичними спостереженнями за кількістю запитів до інформаційної системи можна визначити момент початку кібератаки на сайт підприємства, що працює в режимі електронної комерції.

2. Статистика втрат інших підприємств, що працюють у режимі електронної комерції, дозволять визначити тарифну нетто-ставку та не тільки зменшити ризик електронної комерції, але й зменшити страхові внески.

3. Наведені методики повністю готові до використання комерційними підприємствами тому що мають чітко формалізований і методично вивірений підхід до вирішення проблеми безпеки в електронній комерції.

4. Необхідно продовжити дослідження в напрямі визначення статистики втрат від зловмисних дій та статистики кібератак для підприємств, що працюють у режимі електронної комерції.

Список літератури / References

1. Безопасность электронной коммерции [Електронний ресурс] – режим доступу: http://www.klerk. ru/soft/articles/6795/

"Security of e-commerce", (2004), available at: http://www.klerk.ru/soft/articles/6795/, (accessed February 26, 2014).

2. Ананько А. Заключение договоров путем электронного обмена данными [Електронний ресурс] / А. Ананько – режим доступу: http://www.rassianlaw.net/law/doc/a123.htm.

Ananko A., (2001), "The conclusion of contracts by electronic data interchange", available at: http://www. russianlaw. net/law/edoc/esign/a123/, (accessed February 26, 2014).

3. Виноградська А. Основи підприємництва / Виноградська А.; 2-е вид., перероб. і доп. – К.: Кондор, 2005. – 540 с.

Vynohradska, A. (2005), *Osnovy pidpryiemnytstva* [Fundamentals of Entrepreneurship], Kondor, Kyiv, Ukraine.

4. Волокитина А.В. Электорнная коммерция / Волокитина А.В.; Под ред. Реймана Л.Д. – М.: НТЦ ФИОРД-ИНФО, 2002. – 250 с.

Volokitina, A.V. (2002), *Elektronnaya kommertsyya* [E-Commerce], NTC FIORD-INFO, Moscow, Russia.

5. Глоссарий по информационному обществу [Електронний ресурс] – режим доступу: //http://www.ijs. ru/glossary.

Glossary on Information Society, available at: http://www.ijs.ru/glossary, (accessed February 26, 2014).

6. Интернет. Энциклопедия / Под ред. Л. Мелиховой. – СПб.: Питер, 2001. – 520 с.

Melikhova. L. (2001), *Internet. Entsyklopedia* [Internet. Encyclopedia], Piter, St.-Petersburg, Russia.

7. Гнеденко Б.В. Курс теории вероятностей / Гнеденко Б.В. – М.: Наука, 1998. – 449 с.

Gnedenko, B.V. (1998), *Kurs teorii veroyatnostey* [Course on Probability Theory], Nauka, Moscow, Russia.

8. Пістунов І.М. Актуарні розрахунки / Пістунов І.М. – Дніпропетровськ, РВК НГУ, 2004. – 164 с

Pistunov, I.M. (2004), *Aktuarni rozrakhunky* [Actuarial Calculations], Tutorial, RVK NHU, Dnipropetrovsk, Ukraine.

Цель. Компенсация риска при деятельности коммерческого учреждения, которое работает в режиме электронной коммерции, в направлении его уменьшения, определения основных направлений среди неорганизационных мероприятий.

Методика. Применены методы теории вероятностей, математической статистики и актуарных расчетов.

Результаты. Показано, что статистика запросов к информационной системе, обслуживающей электронную коммерцию предприятия, а также статистика потерь от действий других лиц для предприятий, работающих в этой области, позволяет уменьшить риск. Определены следующие основные направления уменьшения рисков в электронной коммерции как определение момента начала кибератаки и страхование электронной коммерции. Применив методы теории вероятности в предположении, что количество запросов к информационной системе подлежит экспоненциальному закону распределения, удалось рассчитать, что, при превышении на 50% количества запросов, вероятность того, что началась кибератака составляет 0,9. Применение методов, привлеченных из актуарных расчетов, в предположении, что этот тип страхования относится к рисковому, была определена величина нетто-ставки при страховании рисков электронной коммерции путем статистических исследований рынка.

Научная новизна. Расчет критической величины запросов на сайт для определения начала кибератаки является оригинальной разработкой и имеет научную новизну. Оригинальной также есть методика определения нетто-ставки при страховании электронной коммерции.

Практическая значимость. Положения статьи готовы для немедленного использования в работе структур, которые занимаются безопасностью электронной коммерции.

Ключевые слова: *безопасность, электронная коммерция, кибератака, страхование*

Purpose. Risk management in e-commerce enterprises with the purpose of the risk reduction and determination of the main non-organization measures.

Methodology. The methods of probability theory, mathematical statistics and actuarial calculations have been used.

Findings. We have shown that analysis of the statistics of queries to the information system that serves e-commerce companies, as well as statistics of losses from alios acta for companies working in this field can reduce the risk. We have identified the following main ways of e-commerce risks reduction: definition of the beginning of a cyber-attack and e-commerce insurance. We have applied the methods of probability theory assuming that the number of requests to the information system is subject to exponential distribution law and calculated that when the number of requests rises by 50% the probability that the cyber-attack begins is 0.9. The use of techniques borrowed from actuarial calculations, assuming that this case can be

considered as a risk insurance type, allowed us to determine the value of the net rate for e-commerce risk insurance through statistical market research.

Originality. Calculation of the critical number of queries to the site to determine the beginning of cyber-attacks is original and has scientific novelty. The proposed method of determination of the net rate for e-commerce risk insurance is original.

Practical value. All provisions presented in the article are ready for immediate implementation by structures dealing with security of e-commerce.

Keywords: *security, e-commerce, cyber attacks, insurance*

Рекомендовано до публікації докт. екон. наук М.С. Пашкевич. Дата надходження рукопису 06.02.14.

УДК 004.93’1

О.С. Меняйленко[1], д-р техн. наук, проф.,
О.І. Захожай[2], канд. техн. наук, доц.

1 – Луганський національний університет ім. Тараса Шевченка, м.Луганськ, Україна, e-mail: menyaylenko2 @gmail.com
2 – Донбаський державний технічний університет, м.Алчевськ, Україна, e-mail: zoi@bk.ru

ОСНОВИ СИНТЕЗУ КЛАСИФІКАТОРІВ ТЕХНІЧНИХ СИСТЕМ РОЗПІЗНАВАННЯ ОБРАЗІВ З ВИКОРИСТАННЯМ МОДЕЛЕЙ ЕМОЦІЙНИХ ПРОЦЕСІВ ЛЮДИНИ

A.S. Meniailenko[1], Dr. Sci. (Tech.), Prof.,
O.I. Zakhozhay[2], Cand. Sci. (Tech.), Assoc. Prof.

1 – Luhansk Taras Shevchenko National University, Luhansk, Ukraine, e-mail: menyaylenko2@gmail.com
2 – Donbass State Technical University, Alchevsk, Ukraine, e-mail: zoi@bk.ru

SYNTHESIS FUNDAMENTALS OF CLASSIFIERS FOR TECHNICAL SYSTEMS OF PATTERNS RECOGNITION WITH THE USE OF HUMAN’S MODELS OF EMOTIONAL PROCESSES

Мета. Розвиток методики використання емоційних процесів, на кшталт людини, у технічних системах розпізнавання образів з метою підвищення достовірності та зниження часової складності класифікації.

Методика. Проведений аналіз доцільності використання різноманітних емоційних процесів при побудові класифікаторів технічних систем розпізнавання образів. Запропонована інформаційна модель пам’яті людини, яка узагальнена для технічних інтелектуальних систем розпізнавання образів і є розвитком концепції Аткінсона-Шифріна щодо ранжирування інформації за часом зберігання. Розглянута концепція використання емоційних складових в алгоритмах класифікації комбінованих систем розпізнавання образів. Визначені напрями подальших досліджень щодо вдосконалення методики побудови класифікаторів з використанням емоційних процесів.

Результати. Порівняльний аналіз штучних інтелектуальних систем з інтелектуальним апаратом людини вказав на невідповідність результатів класифікації, пов’язану з додатковими емоційними аспектами, що не враховуються. Запропонована інформаційна модель пам’яті людини, яка є узагальненням моделі Аткінсона-Шифріна стосовно технічних систем розпізнавання. Для систем розпізнавання, за аналогією з когнітивним апаратом людини, запропоноване вдосконалення моделі пам’яті через введення характеристик опису емоційних процесів. Це дозволяє здійснити ранжирування ознак об’єктів розпізнавання для їх розміщення в короткочасній пам’яті. Кількісні оцінки емоційних характеристик пропонується визначати як диференціал цільової функції за кожним окремим інформаційним каналом. Встановлено, що у випадку використання комбінованих систем розпізнавання образів доцільне співставлення характеристик емоційних процесів за різними інформаційними каналами.

Наукова новизна. Запропонована інформаційна модель пам’яті людини, яка є узагальненням моделі Аткінсона-Шифріна стосовно технічних систем розпізнавання, до яких вводяться характеристики опису емоційних процесів. Запропонована методика кількісного визначення рівня емоційних процесів у технічних системах розпізнавання образів. Визначена концепція використання емоційних процесів у комбінованих системах розпізнавання образів.

Практична значимість. Використання запропонованих рішень дозволяє ввести до технічних систем розпізнавання образів раціональний набір емоційних складових, що у визначених умовах дозволяє підвищити достовірність класифікації та знизити часову складність цього процесу.

Ключові слова: *модель пам’яті, емоційні процеси в технічних системах, системи розпізнавання образів*

Вступ. Системи розпізнавання образів широко використовуються в різноманітних сферах людської діяльності. Це пов’язане, насамперед, з тим, що відсутність необхідності повного аналітичного представлення всіх закономірностей поведінки об’єктів створює сприятливі умови для прийняття рішень в

© Меняйленко О.С., Захожай О.І., 2015