Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпропетровський державний аграрно-економічний університет

№ 5, 2014 Назад Головна

УДК 336.7

О. В. Черевко ,
д. е. н., доцент, Голова спостережної ради ПАТ «Банк «Київська Русь»

ТЕОРЕТИЧНІ ЗАСАДИ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КЛАСИФІКАЦІЯ ЗАГРОЗ СИСТЕМІ ІНФОРМАЦІЙНОГО ЗАХИСТУ

A. Cherevko,
Ph.D., Associate Professor,
Chairman of the Supervisory Board of PJSC "Bank "Kievan Rus"

THE THEORETICAL BASIS OF THE CONCEPT OF INFORMATION SECURITY THREATS AND CLASSIFICATION OF INFORMATION SECURITY

В статті представлено завдання забезпечення інформаційної безпеки, як одного із головних в сучасному інформаційному суспільстві. Розкрито сутність поняття інформаційної безпеки, основні принципи її забезпечення. Розглянуто класифікацію можливих загроз та заходи щодо усунення цих загроз для інформаційних систем.

In the article the problem of information security as one of the most important in today's information society. The essence of the concept of information security, the basic principles of software. We consider the classification of possible threats and measures to address these threats to information systems.

Ключові слова: *інформація, інформаційна безпека, концепція безпеки, політика інформаційної безпеки, загрози, комп'ютерна система.*

Keywords: *information, information security, the concept of security, policy information security, threats, computer system.*

Постановка проблеми. В сучасному суспільстві саме інформація стає найважливішим стратегічним ресурсом, основною виробничою силою, що забезпечує його подальший розвиток. Ось чому, подібно будь-яким іншим традиційно існуючим ресурсам, інформація також потребує особливого захисту. Поряд з терміном «захист інформації» також широко використовується термін "інформаційна безпека". Якщо захист інформації характеризує процес створення умов, що забезпечують необхідну захищеність інформації, то інформаційна безпека відображає досягнутий стан такої захищеності.

Проблема інформаційної безпеки набула особливої значущості в сучасних умовах широкого застосування автоматизованихних інформаційних систем, заснованих на використанні компютерних і телекомунікаційних засобах. При забезпеченні інформаційної безпеки стали цілком реальними загрози, викликані навмисними (зловмисними) діями людей. Перші повідомлення про факти несанкціонованого доступу до інформації були повязані, в основному, з хакерами, або «електронними розбійниками». Останнім десятиліттям порушення захисту інформації прогресує з використанням програмних засобів і через глобальну мережу Інтернет. Досить поширеною загрозою інформаційної безпеки стало також зараження комп'ютерних систем так званими вірусами.

Таким чином, у зв'язку із зростаючою роллю інформаційних ресурсів в житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема інформаційної безпеки вимагає до себе постійної і більшої уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставини, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, приводять до необхідності комплексного підходу при вирішенні даної проблеми.

Аналіз останніх досліджень та публікацій. Серед праць, котрі присвячені дослідженням методологічних, сутнісних та змістовних основ інформаційної безпеки особливе місце займають теоретичні розробки Е. Бєляєва, М. Бусленка, С. Гринєєва, О. Данильяна, О. Дзьобаня, Г. Ємельянова, В. Лопатіна, О. Позднякова, Л. Сергієнка, В. Циганкова, М. Чеснокова та інших дослідників. Авторами робіт у яких розкриваються особливості забезпечення інформаційної безпеки є праці О.Дзьобаня, А.Колодюка, В.Копилова, А.Кубишкіна, Є.Мануйлова, В.Ніцевича, А.Стрельцова, М.Якушева та ін.

Мета статті. Головними питаннями даного дослідження стали розгляд, з теоретичної точки зору, понять інформаційна безпека та система безпеки інформаційної безпеки. Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій», правомірно було б визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мети, а також інші умови і дії, що порушують безпеку . Розглянуто і заходи захисту інформації від неправомірних дій, які класифіковано за способами здійснення.

Виклад основного матеріалу дослідження. Інформаційна безпека - це стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану. Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту [4]. Для побудови та ефективної експлуатації СЗІБ (система забезпечення інформаційної безпеки) необхідно:

- виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
- врахувати вимоги національного та міжнародного законодавства;
- використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;
- визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;
- рас проділити між підрозділами області відповідальності у здійсненні вимог СЗІБ;
- на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові політики інформаційної безпеки об'єкта захисту;
- реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;
- реалізувати систему менеджменту (управління) інформаційної безпеки (СМІБ);
- використовуючи систему управління організувати регулярний контроль ефективності СЗІБ і при необхідності перегляд і коригування СЗІБ .

Під системою безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво

важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз (Рис. 1.) [2].

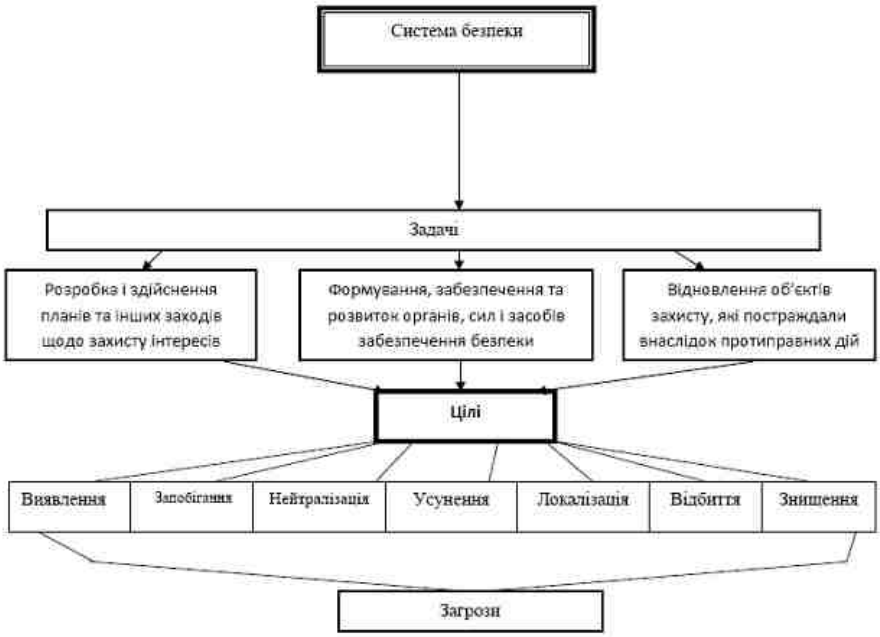

Рис. 1. Функціональна система інформаційної безпеки

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та мети, а також інші умови і дії, що порушують безпеку . При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку [4].

Загроза - сукупність факторів та умов, що виникають в процесі взаємодії об'єкта безпеки з іншими об'єктами, а також складових його компонентів між собою і здатних чинити на нього негативний вплив. Вона виступає в якості можливості вирішення протиріччя у взаємодії об'єкта безпеки з іншими об'єктами, компонентів об'єкта безпеки, що у стадії дисгармонії чи конфлікту, шляхом насильницької зміни в бік погіршення властивостей об'єкта безпеки, або його компонентів, тобто шляхом нанесення шкоди.

Між загрозою і небезпекою нанесення шкоди завжди існують відносини заподіяння, які визначаються як обумовлена сутністю взаємодіючих об'єктів, елементів системи, зв'язок між явищами, при якій одне явище, зване причиною, за наявності певних умов неминуче породжує, викликає до життя інше явище, зване слідством. Загроза завжди породжує небезпеку. Небезпека може бути визначена як стан, в якому знаходиться об'єкт безпеки внаслідок появи загрози. Відмінність між ними полягає в тому, що небезпека є властивістю об'єкта безпеки, а загроза - властивістю об'єкта взаємодії або знаходяться у взаємодії елементів об'єкта безпеки, виступаючих як джерело загроз. Загроза знаходиться у відношенні заподіяння не тільки з небезпекою, але і з очікуваним шкодою - наслідками негативної зміни умов існування, які необхідно подолати для відновлення необхідних умов - в тому сенсі, що очікуваний шкоду визначає величину небезпеки [3] .

Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Види загроз інформаційній безпеці дуже різноманітні і мають безліч класифікацій (наведених в рис. 2):

Рис. 2. Види загроз інформаційної безпеки

Відповідно до наведеної вище класифікації загроз за видом об'єкта впливу вони поділяються на загрози власне інформації, загрози персоналу об'єкта та загрози діяльності щодо забезпечення інформаційної безпеки об'єкта. При більш детальному розгляді загроз інформації, їх можна поділити на загрози носіям конфіденційної інформації, місцям їх розміщення (розташування), каналам передачі (системам інформаційного обміну), а також інформації, що зберігається в документованому (електронному) вигляді на різних носіях. За характером порушення, як один із варіантів класифікації, зображено на рис. 3.

Таким чином, можна зробити висновок про те, що дія загроз інформаційній безпеці об'єкта направлено на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації.

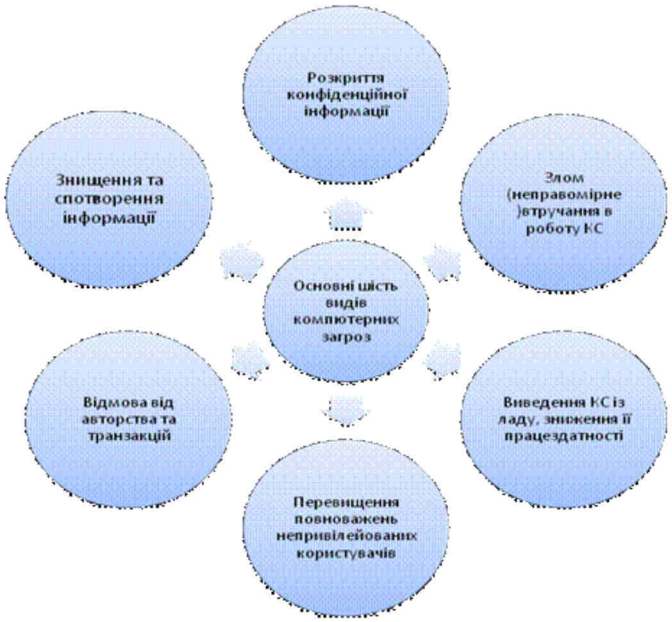

Рис. 3. Шість основних загроз інформаційній безпеці (класифікація за характером порушення)

Одне з ключових понять в оцінці ефективності прояви загроз об'єкту інформаційної безпеки - збиток, що наноситься цьому об'єкту (підприємству) в результаті впливу загроз. За своєю суттю будь-який збиток, його визначення та оцінка мають яскраво виражену економічну основу. Не є винятком і збиток, що наноситься інформаційній безпеці об'єкта (підприємства).

З позиції економічного підходу, загальний збиток інформаційної безпеки підприємства складається з двох складових частин: прямого і непрямого збитку. Прямий збиток інформаційної безпеки підприємства виникає внаслідок витоку конфіденційної інформації. Непрямий збиток - втрати, які несе підприємство у зв'язку з обмеженнями на поширення інформації, в установленому порядку віднесеної до категорії конфіденційної. Опис збитку, що наноситься підприємству в результаті витоку конфіденційної інформації, грунтується на його кількісних і якісних показниках, які базуються на одному з принципів засекречування інформації (віднесення її до категорії конфіденційної) - принципі обгрунтованості. Він полягає у встановленні (шляхом експертних оцінок) доцільності засекречування конкретних відомостей, а також ймовірних наслідків цих дій, з урахуванням розв'язуваних підприємством задач і поставлених цілей.

Введення обмежень на поширення інформації (у зв'язку з її засекречуванням або віднесенням до категорії конфіденційної) призводить і до позитивних, і до негативних наслідків. До основних позитивних наслідків слід віднести запобігання можливого прямого збитку інформаційної безпеки підприємства через витік інформації, що захищається. Негативні наслідки пов'язані з наявністю (ймовірним зростанням) непрямого збитку або витрат у вигляді витрат на захист інформації та величини упущеної вигоди, яка може бути отримана при її відкритому розповсюдженні.

Загальний збиток безпеки підприємства від витоку конфіденційної інформації визначають наступним чином. Проводять класифікацію всіх наявних на підприємстві відомостей за ступенем їх важливості. З цією метою методом експертної оцінки з залученням фахівців структурних підрозділів підприємства, що беруть участь у виконанні робіт з різних напрямків його діяльності, розробляють єдину шкалу відомостей, що містять конфіденційну інформацію - так званий рейтинг важливості інформації. У рейтингу відбиваються всі відомості, включені до переліків інформації, що підлягає захисту[3].

Методичною основою для розробки такого рейтингу служить метод експертного аналізу в сукупності з методом об'єктивного кількісного оцінювання. На основі рейтингу важливості інформації зіставляють (співвідносять) включені до нього відомості з кількісними показниками можливого збитку, що визначається розрахунковим або експертним шляхом.

При розробці необхідних, засобів, методів і заходів, що забезпечують захист інформації, необхідно враховувати велику кількість різних факторів.

Інформація, будучи предметом захисту, може бути представлена на різних технічних носіях. Її носіями можуть бути люди з числа користувачів і обслуговуючого персоналу. Інформація може піддаватися обробці в комп'ютерних системах, передаватися по каналах зв'язку і відображатися різними пристроями. Вона може розрізнятися за своєю цінністю. Об'єктами, що підлягають захисту, де може перебувати інформація, є не тільки комп'ютери і канали зв'язку, але й приміщення, будівлі та прилегла територія. Істотно різнитися може кваліфікація порушників, а також використовувані способи і канали несанкціонованого доступу до інформації. Таким чином, основними принципами забезпечення інформаційної безпеки є наступні[5]:

Системності.

Комплексності.

Безперервності захисту.

Розумної достатності.

Гнучкості управління і застосування.

Відкритості алгоритмів і механізмів захисту.

Простоти застосування захисних заходів і засобів.

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем підрозділяють на:

правові (законодавчі);

морально-етичні;

організаційно-адміністративні;

фізичні;

апаратно-програмні.

До *правових заходів* захисту інформації належать діючі в країні закони, укази, положення, інструкції та інші нормативні акти, які регламентують правила поводження з інформацією обмеженого використання і відповідальності за їх порушення. Цим вони перешкоджають несанкціонованому використанню інформації і є стримуючим фактором для потенційних порушників[5].

До *морально-етичним* заходам протидії відносяться всілякі норми поведінки, які традиційно склалися або складаються в суспільстві у міру поширення комп'ютерів в країні. Ці норми бувають як неписаними (загальновизнані норми чесності, патріотизму і т.д.), так і оформленими в якийсь звід правил чи приписів.

Організаційно-адміністративні заходи захисту регламентують процеси функціонування ІС(інформаційних систем); використання ресурсів ІС; діяльність персоналу інформаційної служби на підприємтсві; порядок взаємодії користувачів із системою, з тим, щоб найбільшою мірою утруднити чи виключити можливість реалізації загроз безпеці.

Організаційно-адміністративні заходи включають в себе :

розробку правил обробки інформації в ІС;

сукупність дій при проектуванні та обладнанні обчислювальних центрів та інших об'єктів ІС (облік впливу стихії, пожеж, охорона приміщень тощо);

сукупність дій при підборі й підготовці персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки; створення умов, при яких персоналу було б невигідно допускати зловживання тощо);

організацію надійного пропускного режиму;
організацію обліку, зберігання, використання та знищення документів і носіїв з конфіденційною інформацією;
розподіл реквізитів розмежування доступу (паролів, повноважень тощо);
організацію прихованого контролю за роботою користувачів і персоналу ІС;
сукупність дій при проектуванні, розробці, ремонті та модифікації устаткування і програмного забезпечення (сертифікація використовуваних технічних і програмних засобів, суворе санкціонування, розгляд і затвердження всіх змін, перевірка на задоволення вимогам захисту, документальна фіксація змін тощо).

До *фізичних мір* захисту відносяться різні механічні, електро- і електромеханічні пристрої або споруди, спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу порушників (турнікети, колючий дріт, кодові замки, системи охоронно-пожежної сигналізації тощо).

До *апаратно-програмним заходам* захисту відносяться різні електронні пристрої та спеціальні програми, які реалізують самостійно або в комплексі з іншими засобами наступні способи захисту[5]:
ідентифікацію і аутентифікацію суб'єктів ІС;
розмежування доступу до ресурсів ІС;
контроль цілісності даних;
забезпечення конфіденційності даних;
аудит подій, що відбуваються в ІС;
резервування ресурсів і компонентів ІС.

Висновки. Отже, в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованої, конкретної, активної, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Література.

1. Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. - М.: МГИУ, 2005. - 215 с.
2. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.
3. Конев И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.
4. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.
5. И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина Теория информационной безопасности и методология защиты информации // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008 с. 358.
6. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы [Электронный ресурс]. – Режим доступа : http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.
7. Курушин В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – М. : Новый юрист. – 2012. – 256 с.
8. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – СПб. : СПбГУ ИТМО, 2010. – 98 с.
9. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с.
10. Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

References.

1. Semenenko, V.A. (2005), *Informacionnaja bezopasnost'* [Information security], MGIU, Moscow, Russia.
2. Kornjushin, P.N. (2003), *Informacionnaja bezopasnost'* [Information security], TIDOT DVGU, Vladivostok, Russia.
3. Konev, I.R. (2003), *Informacionnaja bezopasnost'* [Information security], BHV-Peterburg, Saint Petersburg, Russia.
4. Kavun, S.V. (2008), *Informatsijna bezpeka* [Information security], Vyd. KhNEU, Kharkiv, Ukraine.
5. Anikin, I.V. Glova, V.I. Nejman, L.I. Nigmatullina, A.N. (2008), *Teorija informacionnoj bezopasnosti i metodologija zashhity informacii* [The theory of information security and protection of information methodology], Izd-vo Kazan. gos. tehn. un-ta, Kazan, Russia.
6. Sorokovskaja, A.A. (2010), "Information security company: new threats and prospects", available at: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf (Accessed 28 April 2014).
7. Kurushin, V.D. and Mynaev, V. A. (2012), *Komp'juternye prestuplenija i informacionnaja bezopasnost'* [Computer crimes and information security], Novyj jurist, Moscow, Russia.
8. Gatchin, Ju.A. (2010), *Teorija informacionnoj bezopasnosti i metodologija zashhity informacii* [The theory of information security and protection of information methodology], SPbGU ITMO, Saint Petersburg, Russia.
9. Hajvorons'kyj, M.V. and Novikov, O.M. (2009), Bezpeka informatsijno-komunikatsijnykh system [Safety of information and communication systems], Vydavnycha hrupa BHV, Kyiv, Russia.
10. Dron', M.M. Malajchuk, V.P. and Petrenko, O.M. (2001), *Osnovy teorii zakhystu informatsii* [Bases of the theory of information protection], Vyd-vo Dnipropetr. un-tu, Dnipropetrovsk, Ukraine.

Стаття надійшла до редакції 18.05.2014 р.