УДК 65.012.8+342.951:007

Анфіса Нашинець-Наумова,

канд. юрид. наук, доцент,
доцент кафедри правознавства
Інституту суспільства Київського університету імені Бориса Грінченка

ОРГАНІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Захист інформації є одним із найважливіших складників інформаційної безпеки суб'єктів господарювання. У статті проаналізовано основні етапи створення системи інформаційної безпеки, класифіковано й розкрито причини витоку інформації, запропоновано шляхи забезпечення захисту інформації в системі інформаційної безпеки. Акцентовано увагу на основних проблемах, які перешкоджають організації ефективної системи захисту інформації суб'єктів господарювання.

Ключові слова: інформаційна безпека суб'єктів господарювання, система захисту інформації, інформація з обмеженим доступом, загроза безпеці інформації.

Постановка проблеми. Сьогодні інформація вважається стратегічним національним ресурсом – одним з основних багатств країни. Під впливом інформатизації всі сфери життя суспільства набувають нових якостей: гнучкості, динамічності тощо. Однак водночас зростає й потенційна вразливість суспільних процесів від інформаційного впливу. Д. Паркер, міжнародний експерт із питань інформатики, вважає, що на зміну небезпеці виникнення ядерної катастрофи може прийти загроза розв'язання війни, яка прийме нові форми [1, с. 23]. Це буде боротьба, спрямована проти країн, які володіють передовими технологіями, з метою створення хаосу в інформаційних структурах і спричинення економічної катастрофи. Інші експерти стверджують, що збір економічної інформації про конкурентів і захист власних інформаційних ресурсів – головні завдання забезпечення безпеки економіки. Західні фахівці впевнені, що в разі повного розсекречення комп'ютерної інформаційної мережі більшість компаній буде знищено конкурентами за дуже короткий проміжок часу.

З огляду на те, що інформаційна безпека на межі ІІІ тисячоліття виходить на перше місце в системі національної безпеки, формування й проведення єдиної державної політики в цій сфері вимагає пріоритетного розгляду. Сьогодні склались дві тенденції в органах державної влади у визначенні поняття та структури інформаційної безпеки. Представники гуманітарного напряму пов'язують інформаційну безпеку лише з інститутом таємниці. Представники силових структур пропонують поширити сферу інформаційної безпеки практично на всі питання й відносини в інформаційній сфері, фактично ототожнюючи інформаційну безпеку з інформаційною сферою. Істина, як завжди, лежить посередині.

Сьогодні став популярним такий афоризм: «Хто володіє інформацією, той володіє світом». Інформаційна безпека суспільства й держави характеризується ступенем їх захищеності, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості тощо) щодо небезпечних, дестабілізуючих, деструктивних дій, які шкодять інтересам країни.

Отже, під захистом інформації розуміється комплекс заходів, які здійснюються власником інформації щодо виокремлення своїх прав на володіння й розпорядження інформацією, створення умов, які обмежують її поширення, виключають чи суттєво ускладнюють несанкціонований, незаконний доступ до таємної інформації та її носіїв. Інформація, що захищається, може містити дані, які належать до різних охоронюваних законом таємниць. Цілком природно, що кожний вид інформації, який охороняється, може мати свої особливості у сфері регулювання організації та здійснення захисту [2, с. 173].

Аналіз останніх досліджень і публікацій. Сучасним науковим розвідкам, присвяченим проблематиці інформаційної безпеки, у тому числі у сфері організації системи захисту інформації суб'єктів господарювання (їх авторами є І. Арістова, І. Бачило, В. Брижко, В. Гавловський, Р. Калюжний, В. Копилов, В. Ліпкан, А. Марущак, В. Цимбалюк,

М. Швець, Ю. Шемшученко та інші вчені), притаманна відсутність широкої різноманітності поглядів на окреслену проблему.

Метою статті є виділення й аналіз етапів забезпечення захисту інформації суб'єктів господарювання з огляду на правове регулювання цієї сфери відносин в Україні.

Виклад основного матеріалу. Деякі науковці вважають, що захист інформації є цілеспрямованою діяльністю власників інформації, спрямованою на виключення чи суттєве обмеження можливостей витоку, нав'язування, блокування або знищення інформації, що підлягає захисту [3, с. 126]. Одним із можливих шляхів наукового пошуку в обраному напрямі є дослідження захисту інформації як системи, тобто як цілісного утворення, що цікавить нас у своїй єдності, причому варто пам'ятати, що будь-який об'єкт становить систему лише щодо певної мети [4, с. 7].

З позиції теорії управління на загальному рівні система складається з керуючого й керованого об'єкта та створюється з урахуванням заданих вимог і наявних обмежень [3, с. 128].

Система може нормально функціонувати лише за наявності в ній певних зв'язків між об'єктом управління та управлінським об'єктом. Обов'язковою умовою для нормального функціонування системи є наявність зворотного зв'язку. Загалом для функціонування будь-якої системи необхідні насамперед збуджувальні фактори, які можуть бути наслідком зовнішнього впливу або внутрішньої незадоволеності поточним станом справ.

Зауважимо, що відповідно до системного підходу, застосованого в науковій літературі, закономірності цілого (системи) безумовно домінують над її компонентами. Однак роль складників не варто зводити до становища суто пасивних частин. Будучи залежними від системи як цілого, компоненти мають певну відносну самостійність [5, с. 13].

Розглянемо динаміку функціонування системи захисту інформації на рівні суб'єкта господарювання – організації, яка працює з інформацією з обмеженим доступом. Оскільки будь-яка система створюється для вирішення певного кола завдань, то у своєму функціонуванні вона обмежується як об'єктивними, так і суб'єктивними чинниками. До цих чинників належать такі:

– переліки захищених відомостей, що складають державну чи комерційну таємницю;

– необхідні рівні безпеки інформації, забезпечення яких не приведе до перевищення збитків над витратами щодо захисту інформації;

– загрози безпеці інформації;

– показники, за якими оцінюватиметься ефективність захисту інформації [3, с. 120].

Входами системи захисту інформації є такі явища:

1) вплив зловмисників у процесі фізичного проникнення до місцезнаходження джерел конфіденційної інформації з метою її викрадення, внесення змін або знищення;

2) різноманітні фізичні поля, електромагнітні сигнали, які створюються технічними засобами зловмисників і впливають на засоби обробки й збереження інформації;

3) стихійні лиха (насамперед пожежі), що призводять до знищення або перекручування інформації;

4) фізичні поля та електричні сигнали з інформацією, які передаються функціональними каналами зв'язку;

5) побічні електромагнітні наведення й акустичні поля, а також електричні сигнали, що виникають у процесі діяльності об'єктивного захисту та несуть у собі конфіденційну інформацію.

Виходами системи є заходи щодо захисту інформації, адекватні вхідним впливам. Алгоритм процесу перетворення вхідних впливів (загроз) на заходи захисту визначає варіант системи захисту.

Побудова системи захисту інформації суб'єкта господарювання здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування та керування системою захисту інформації [6].

На першому етапі побудови системи захисту інформації необхідно здійснити аналіз об'єктивного захисту, ситуаційного плану, умов функціонування підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз.

Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні чи ненавмисні дії юридичних і фізичних осіб.

На другому етапі побудови системи захисту інформації варто скласти план захисту інформації, що містить організаційні, первинні технічні та основні технічні заходи захисту інформації з обмеженим доступом, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог захисту інформації для всіх

періодів життєвого циклу об'єкта захисту. Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів технічного захисту інформації (далі – ТЗІ). Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

Для технічних засобів інформації необхідно застосовувати спосіб приховування або спосіб технічної дезінформації.

Заходи захисту інформації повинні відповідати загрозам; розроблятись з урахуванням можливої шкоди від їх реалізації й вартості захисних заходів та обмежень, що вносяться ними; забезпечувати задану ефективність захисту інформації на встановлені рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень захисту інформації визначається системою кількісних і якісних показників, які забезпечують вирішення завдання захисту інформації на основі норм і вимог ТЗІ. Мінімально необхідний рівень захисту інформації забезпечується обмежувальними й фрагментарними заходами протидії найнебезпечнішій загрозі. Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

Порядок розрахунку та інструментів визначення заходів безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту й порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) встановлюються нормативними документами системи ТЗІ.

На третьому етапі побудови системи захисту інформації необхідно реалізувати організаційні, первинні технічні й основні технічні заходи захисту інформації з обмеженим доступом, встановити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) на відповідність вимогам безпеки інформації [7, с. 31–35].

Надання послуг із ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні й фізичні особи, які мають ліцензію на право проведення цих робіт, видану уповноваженим Кабінетом Міністрів України органом.

На четвертому етапі побудови системи захисту інформації варто провести аналіз функціонування системи захисту інформації, перевірку виконання заходів технічного захисту інформації, контроль ефективності захисту, підготувати й видати дані для керування системою захисту інформацією.

Керування системою захисту інформації полягає в адаптації заходів ТЗІ до поточного захисту.

За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізовуються в найкоротший строк. У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені першим, другим і третім етапами побудови системи захисту інформації. Порядок проведення перевірок та контролю ефективності захисту інформації встановлюється нормативними документами.

Таким чином, захист інформації має передбачати її збереження від широкого кола різноманітних загроз, таких як витік інформації, несанкціоновані й ненавмисні впливи тощо. Нормативні документи сфери ТЗІ під загрозою пропонують розуміти витік, можливість блокування чи порушення цілісності інформації [8].

Сучасною науковою думкою категорія «загроза безпеці інформації» визначається як виникнення такого явища чи події, наслідком яких може бути негативний вплив на інформацію: порушення фізичної цілісності, логічної структури, несанкціонована кодифікація, несанкціоноване отримання, несанкціоноване розмноження [9, с. 93].

Нині фахівцями досліджуються численні різнопланові загрози різноманітного походження. Упродовж усього періоду існування проблеми захисту інформації здійснювалися спроби класифікації джерел загроз безпеці інформації та самих загроз із метою подальшої стандартизації засобів і методів, що застосовуються для захисту. Різними авторами було запропоновано низку підходів до такої класифікації [10; 11; 12]. Причому як критерії розподілу сукупності загроз за класами використовуються види небезпек, що викликані вказаними загрозами, ступінь умислу, джерело походження тощо.

У відомій монографії Л. Хоффмана «Сучасні методи захисту інформації» [13] було виділено 5 груп різноманітних загроз: викрадення носіїв, запам'ятовування або копіювання інформації, несанкціоноване підключення до апаратури, несанкціонований доступ до ресурсів системи, перехоплення побічних електромагнітних випромінювань і наведень.

Автори науково-практичного посібника «Захист інформації в персональних ЕОМ» [14] як критерій класифікації обрали тип засобу, за допомогою якого може бути реалізовано несанкціоноване отримання інформації, та виділили 3 типи таких засобів: людину, техніку й програмне забезпечення. До групи загроз, у реалізації яких провідну роль виконує людина, включено викрадення носіїв, читання інформації з екрану дисплея, читання інформації з роздруківок; до групи,

де основними засобами є технічні пристрої, – підключення до техніки й перехоплення випромінювань; до групи, де основним засобом є програмне забезпечення, – несанкціонований програмний доступ, програмне дешифрування зашифрованих даних, програмне копіювання інформації з носіїв.

Аналогічний підхід запропонували автори навчальних посібників із захисту інформації від несанкціонованого доступу [12; 15]. Вони виокремили 3 класи загроз: природні (стихійні лиха, магнітні бурі, радіоактивні випромінювання); технічні (відключення чи коливання електроживлення, відмови й збої апаратно-програмних засобів, електромагнітні випромінювання та наведення; витоки через канали зв'язку); створені людьми (ненавмисні та умисні дії різних категорій осіб).

Ще один вид джерел загроз безпеці інформації, пов'язаний із її викраденням, досить детально класифіковано в монографії С. Расторгуєва [11]. Учений вирізняє такі способи виокремлення інформації:

1) каналами побічних електромагнітних випромінювань;

2) шляхом негласного копіювання, причому йдеться про два різновиди копіювання: «вручну» (друк з екрану на принтер або виведення з пам'яті на принтер чи екран) та «вірусне» (наприклад, виведення з пам'яті на принтер або екран, передача інформації за допомогою вбудованої на комп'ютері радіозакладки);

3) викрадення носіїв інформації;

4) викрадення персонального комп'ютера.

У монографії В. Герасименка [10] введено поняття дестабілізуючих чинників, джерел їх виявлення та причин порушення захищеної інформації. Запропоновано підходи до формування відносно повних множин таких причин і наведено структуру цих множин щодо порушення фізичної цілісності інформації й несанкціонованого її отримання.

Детальний аналіз загроз несанкціонованого отримання інформації наведено також у навчальному посібнику В. Гайковича та Д. Єршова [16], причому концептуальні підходи аналізу аналогічні викладеним у роботі В. Герасименка [10].

Своєрідним видом загроз є спеціальні програми, які приховано й умисно впроваджуються у функціональні програмні системи та після одного чи декількох запусків руйнують інформацію на жорсткому диску комп'ютера або вчиняють інші несанкціоновані дії. Нині відомі численні різновиди таких програмних засобів: електронні віруси, комп'ютерні черви, троянські програми тощо.

Шкідливі програми становлять велику небезпеку для сучасних автоматизованих систем. Детальний аналіз цих загроз і методів боротьби з ними наведено в працях П. Біленчука, Б. Романюка, В. Цимбалюка, А. Новицького та інших учених [17; 18; 19].

Аналіз праць фахівців із питань захисту інформації показує, що в процесі формування множини загроз останнім часом досить чітко виявляється тенденція переходу від емпіричних до системно-концептуальних, науково обґрунтованих підходів [9, с. 95].

Ефективна протидія загрозам інформації досягається винятково за умови комплексного застосування засобів та організаційно-технічних методів із метою захисту охоронюваних відомостей про об'єкт [20, с. 127]. Причому вказані засоби й методи мають застосовуватись відповідно до мети й завдань протидії, етапів життєвого циклу об'єкта та способів протидії.

Суттєвим моментом є необхідність реалізації захисту інформації вчасно, активно, різноманітно, безперервно, раціонально, комплексно й планово.

Одна з основних вимог – вчасність прийняття рішення щодо організації захисту інформації. Процес прийняття рішення потрібно прискорити з певних причин: по-перше, щоб вчасно розв'язати проблеми, що виникли, і не давати їм «розростатись» до такого стану, коли їх вирішення стане неможливим чи марним; по-друге, щоб відповідальні виконавці мали достатньо часу для виконання поставлених перед ними завдань.

Активність протидії передбачає насамперед наступальний, активний її характер, ґрунтується на аналізі обставин, умінні зробити правильні висновки про можливі дії потенційного супротивника, що дадуть змогу запобігти та наполегливо реалізувати ефективні заходи протидії.

Різноманітність протидії спрямовується на унеможливлення шаблонного підходу до організації й проведення заходів і творчий підхід до реалізації заходів щодо захисту інформації.

Комплексність передбачає вжиття комплексу заходів, спрямованих на своєчасне перекриття всіх можливих каналів витоку інформації. Неприпустимим є застосування окремих технічних засобів або методів, спрямованих на захист окремих серед загального числа можливих каналів витоку інформації.

Безперервність протидії – це реалізація заходів щодо комплексного захисту об'єкта інформаційної діяльності на всіх етапах життєвого циклу розроблення й існування спеціальної продукції або забезпечення виробничої діяльності об'єкта захисту.

Плановість реалізації заходів передбачає насамперед передбачені раніше, ще на стадії

проектування й будівництва об'єкта, заходи, спрямовані на захист інформації.

Важливо, щоб заходи з протидії виглядали правдоподібно та відповідали умовам обстановки, виконувались згідно з планами захисту інформації об'єкта. У зв'язку із цим розробляються й реалізовуються практичні заходи щодо маскування захисних заходів.

В основі захисту інформації лежить сукупність правових форм діяльності власника, що реалізується з метою виконання вимог щодо збереження охоронюваних відомостей та інформаційних процесів, а також заходів контролю за ефективністю вжитих заходів щодо захисту інформації [20, с. 128].

Досліджуючи проблеми, пов'язані з організацією захисту інформації, варто зауважити, що такий захист не є окремим, разовим епізодом. Захист має реалізовуватись комплексно й безперервно [6; 21].

Нормативно-правове розуміння адміністративно-правових заходів захисту інформації, у тому числі інформації з обмеженим доступом, зводиться до системи правових, організаційних, інженерно-технічних заходів, які спрямовуються на збереження цілісності службової інформації та запобігання її витоку.

Адміністративно-правові заходи захисту інформації з обмеженим доступом можна визначити як сукупність методів, засобів і прийомів, спрямованих на захист інформаційної безпеки людини, суспільства й держави в усіх сферах життєво важливих інтересів.

Сукупність їх полягає у виявленні, вилученні та нейтралізації негативних джерел, причин та умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації, а цілі й методи адміністративно-правового захисту інформації з обмеженим доступом здійснюються з огляду на її зміст.

Тому зміст адміністративно-правового захисту інформації з обмеженим доступом ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини.

А. Антонюк відносить до сфери безпеки інформації не захист інформації, а захист права власності на неї [22, с. 103]. Справді, захист інформації організовує та здійснює власник, користувач інформації або уповноважена ними особа (фізична чи юридична), а також держава в особі компетентних органів у межах своєї правоохоронної функції. Захистом інформації власник охороняє свої права на володіння й розповсюдження інформації, намагається запобігти незаконному заволодінню нею та використанню її на шкоду власним інтересам. Система захисту може бути різною, на розсуд власника, а може й не мати такого захисту взагалі. Він здійснюється на основі диспозитивних методів, що входять у сферу цивільно-правового розгляду. Захист інформації стає предметом адміністративно-правового регулювання у випадках, коли обмеження доступу до інформації прямо передбачаються законами, коли ці обмеження пов'язуються із забезпеченням інформаційних прав і свобод людини, інформаційних аспектів національної, державної, громадської безпеки тощо, а суб'єктом застосування цих обмежень, що дуже важливо, є держава в особі її компетентних органів [23, с. 103].

Захистінформаціїзобмеженимдоступом– це комплекс дій власника інформації для збереження прав на її володіння й розповсюдження, а також сприяння життєдіяльності людини, суспільства та держави на основі створення органами управління безпечних умов, що обмежують розповсюдження й виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Форми адміністративно-правового захисту інформації з обмеженим доступом традиційно можна класифікувати на юрисдикційні та неюрисдикційні. До перших належить захист порушених прав суб'єктів інформаційних правовідносин у судовому й адміністративному порядку, до других – технічні засоби захисту інформації з обмеженим доступом.

Механізм захисту інформації з обмеженим доступом є повним поєднанням технічних і юрисдикційних засобів захисту інформації. Усі вони є правовими, оскільки встановлюються правовими актами управління, у тому числі нормативно-правовими.

Адміністративно-правове забезпечення інформації з обмеженим доступом – це діяльність щодо застосування юрисдикційних і неюрисдикційних форм її захисту.

Діяльність щодо технічного захисту інформації з обмеженим доступом повинна відповідати таким вимогам:

– наявності спеціальної освіти в осіб, які її здійснюють, або наявності в них спеціальної підготовки;

– відповідності виробничих приміщень, виробничого, випробувального й контрольно-вимірювального устаткування технічним нормам і вимогам, встановленим державними стандартами й нормативно-методичними документами щодо технічного захисту інформації з обмеженим доступом;

– використанню сертифікованих автоматизованих інформаційних систем і засобів їх захисту;

– використанню третіми особами програм для комп'ютерів чи баз даних на підставі договору з їх правовласником.

Юрисдикційні форми реалізації адміністративно-правових заходів захисту інформації з обмеженим доступом у суб'єктів господарювання реалізовуються з метою відновлення порушених прав суб'єктів інформаційних правовідносин. До цих заходів відносимо насамперед такі:

а) віднесення відомостей до інформації з обмеженим доступом;

б) документування інформації з обмеженим доступом, що є основою для реєстрації інформаційних ресурсів;

в) правовий захист інформації з обмеженим доступом, що виражається в існуванні інституту адміністративно-правової відповідальності за порушення законодавства про службову інформацію, який є однією з гарантій належної її реалізації та правового захисту.

Висновки

Таким чином, проблема захисту інформації з обмеженим доступом вбачається в урегулюванні порядку реєстрації баз, банків даних у частині визначення права власності на ці ресурси й порядку обліку їх у складі майна суб'єктів господарювання. Інша проблема щодо захисту інформації з обмеженим доступом – відсутня систематизація адміністративного законодавства в частині об'єднання норм, які встановлюють адміністративно-правову відповідальність за порушення, предметом посягання яких може бути інформація з обмеженим доступом.

Звісно, наведене є далеко не повним переліком проблем, які потребують свого нормативно-правового врегулювання з метою захисту безпеки інформації суб'єктів господарювання. Однак вкрай необхідно запровадити головні засади й принципи, на основі яких можна здійснювати подальший розвиток системи захисту інформації суб'єктів господарювання.

Список використаних джерел

1. Паркер Д. Преемственность и изменение геополитической мысли Запада / Д. Паркер // Международный журнал социальных наук. – 1993. – № 3. – С. 22–30.

2. Государственная тайна и ее защита в РФ : [учеб. пособие] / под общ. ред. М. Вуса и А. Федорова. – 3-е изд., испр. и доп. – СПб. : Изд-во Р. Асланова «Юридический центр Пресс», 2007. – 752 с.

3. Шепета О. Адміністративно-правові засади технічного захисту інформації : дис. ... канд. юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право» / О. Шепета ; Нац. академія Служби безпеки України. – К., 2011. – 215 с.

4. Кузьменко А. «Системный взгляд» на систему права / А. Кузьменко // Известия высших учебных заведений. Серия «Правоведение». – 2003. – № 3. – С. 4–11.

5. Костицька І. Політико-правова природа народного представництва / І. Костицька // Право України. – 2006. – № 10. – С. 9–14.

6. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – К. : Держстандарт України, 1997. – 15 с.

7. Головань С. Про термінологію в області безпеки інформації / С. Головань, А. Давиденко, Л. Щербак // Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г.Є. Пухова. – 2013. – Вип. 66. – С. 31–35.

8. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – К. : Держстандарт України, 1997. – 16 с.

9. Малюк А. Информационная безопасность: концептуальные и методологические основы защиты информации : [учеб. пособие для вузов] / А. Малюк. – М. : Горячая линия, 2004. – 280 с.

10. Герасименко В. Защита информации в автоматизированных системах обработки данных : в 2 кн. / В. Герасименко. – М. : Энергоатомиздат, 1994– . – Кн. 1. – 1994. – 400 с.

11. Расторгуев С. Программные методы защиты информации : [учеб. пособие] / С. Расторгуев. – Пенза : Пензенский гос. ун-т, 2000. – 95 с.

12. Петров В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах / В. Петров, А. Писарев, А. Шейн. – М. : МИФИ, 1995. – 48 с.

13. Хоффман Л. Современные методы защиты информации / Л. Хоффман ; под ред. В. Герасименко. – М. : Советское радио, 1980. – 264 с.

14. Спесивцев А. Защита информации в персональных ЭВМ / А. Спесивцев, В. Венгер, А. Крутяков и др. – М. : Радио и связь ; Веста, 1993. – 192 с.

15. Михайлов С. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции : [учеб. пособие] / С. Михайлов, В. Петров, Ю. Тимофеев. – М. : МИФИ, 1995. – 112 с.

16. Гайкович В. Основы безопасности информационных технологий : [учеб. пособие] / В. Гайкович, Д. Ершов. – М. : МИФИ, 1995. – 96 с.

17. Біленчук Г. Комп'ютерна злочинність : [навч. посібник] / Г. Біленчук, Б. Романюк, В. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.

18. Скородумов Б. Информационная безопасность. Обеспечение безопасности электронных банков : [учеб. пособие] / Б. Скородумов. – М. : МИФИ, 1995. – 104 с.

19. Новицький А. Правове регулювання інституціоналізації інформаційного суспільства в Україні : [монографія] / А. Новицький. – Ірпінь : НУ ДПС України, 2011. – 444 с.

20. Бузов Г. Защита от утечки информации по техническим каналам : [учеб. пособие] / Г. Бузов, С. Калинин, А. Кондратьев. – М. : Горячая линия, 2005. – 416 с.

21. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. – К. : Держстандарт України, 1997. – 11 с.

22. Антонюк А. Основи захисту інформації в автоматизованих системах : [навч. посібник] / А. Антонюк. – К. : Академія, 2003. – 244 с.

23. Марущак А. Інформаційне право: доступ до інформації : [навч. посібник] / А. Марущак. – К. : КНТ, 2007. – 532 с.

Защита информации является одной из важнейших составляющих информационной безопасности субъектов хозяйствования. В статье проанализированы основные этапы создания системы информационной безопасности, классифицированы и раскрыты причины утечки информации, предложены пути обеспечения защиты информации в системе информационной безопасности. Акцентировано внимание на основных проблемах, которые препятствуют организации эффективной системы защиты информации субъектов хозяйствования.

Ключевые слова: информационная безопасность субъектов хозяйствования, система защиты информации, информация с ограниченным доступом, угроза безопасности информации.

Data protection is one of the most important components of information security of business entities. The article analyzes the main steps of creating a system of information security, classified and disclosed the reasons for the leakage of information, the ways of ensuring the protection of information in information security. The attention is focused on the main problems that hinder the organization of an effective system of protection of information entities.

Key words: information security entities, protection system information, information with limited access, data security threat.