організованих асоціацій і заборони мирних зібрань створює перешкоди в реалізації ідеї вільного обміну інформацією. Як вже було відмічено вище, технології в усіх відношеннях і сенсах в рази підсилюють зв'язок права на особисте життя або конфіденційність, описані в статті 12, з правом, проголошеним у статті 19 цього документа, на пошук, отримання і поширення інформації.

У суспільстві сьогоднішнього дня політика та інформаційні технології нерозривно пов'язані. Інформаційно-комунікаційні технології при умові законної реалізації даних можливостей цілком здатні втілити у життя всі пункти статті 21, де зазначено про виборче право кожної людини за допомогою форм, які забезпечують свободу голосування, в іншому випадку необхідно підкреслити, що демократичні вибори втрачають сенс. Прикладом тому можуть служити такі дії, як фальсифікація результатів електронного голосування або виключення значного числа груп виборців зі списку політично активних одиниць шляхом позбавлення доступу до інформаційно-комунікаційних технології і т. д.

Наступна тема стосується освіти в інформаційному суспільстві, яке з впровадженням інформаційних технологій набуває найважливіший статус і значення у соціальному житті людини. Виділимо кілька причин, що визначають залежність сучасної освіти від інформаційних технологій. В першу чергу, зростання цінності технічного навчання, обумовленого масштабним застосуванням технологій в усіх областях. Друга причина полягає в тому, що інформаційні технології – це джерело знань і один із способів взаємодії в науково освітньому середовищі. Тому проблема цифрового розшарування суспільства стає актуальною у сфері здобуття освіти, вирішувати її – важливе державне завдання інформаційного суспільства.

Втілення в життя концепції формування загального інформаційного середовища як джерела поширення творчих ідей – основна мета впровадження та використання інформаційних технологій. Ідеї вільного поширення інформації та захист авторських прав – поле битви зіткнулися інтересів в надрах глобальних мереж. Технічні засоби, що дозволяють повноцінно взаємодіяти в культурному житті, або технології, що порушують інтереси право-володарів?

Так, Декларація прав людини ООН проголосила в якості пріоритетних цілей забезпечення справедливості, свободи і миру. Ідею свободи ми пропонуємо конкретизувати у свободі переконань, совісті, доступу до інформації, ідея справедливості закладена у можливості рівного доступу до інформації, забезпечення миру та криється у праві на участь в управлінні державними процесами, що відбуваються в країні.

Список використаної літератури

1. Этические аспекты новых технологий. Обзор. – М.: Права человека, 2007. – 102 с.
2. Всеобщая декларация прав человека [Электронный ресурс]. URL: http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml.
3. Программы – фильтры для ограничения информации для граждан через Интернет, устанавливаемые государством [Электронный ресурс]. URL: http://www/opennetinitiative.org.

ІНФОРМАЦІЙНА БЕЗПЕКА ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Коломієць А. В.
м. Полтава

У сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і

решта ресурсів, потребує особливого захисту. Проблема інформаційної безпеки набула особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. У зв'язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, приводять до необхідності комплексного підходу при вирішенні цієї проблеми.

Аналіз останніх досліджень і публікацій показує, що загалом інформація пронизує всі сфери життя суспільства, створюючи нову основу розвитку економіки, культури і взагалі нову характеристику соціуму. Вивченням питання інформаційної безпеки займалися такі вчені, як С. Ф. Гуцу, Б. А. Кормич, А. І. Марущак, О. А. Сороківська [1-4]. Класичними чинниками економічної безпеки країни, за визначенням О. А. Кулініч, є «активізація попиту і відповідна за обсягами та структурою реакція пропозиції» [5, с. 59-60]. Учений під класичними чинниками економічної безпеки розуміє чинники сталого економічного зростання, які досліджує через вивчення та порівняння зростання внутрішнього попиту, зміни його структури за секторами та верствами населення. Живко З. Б. та Керницькою М. І. проаналізовано чинники позитивного та негативного, прямого та опосередкованого впливу у різних сферах безпеки, зазначено роль індикаторів і чинників економічної безпеки, визначено та досліджено суть соціально-економічної безпеки [6, с. 14-15].

Кавун С. В. визначає життєвий цикл економічної безпеки підприємства та досліджує основні рівні економічної безпеки підприємства [7, с. 17-18]. Однак у комплексі чинники інформаційної безпеки підприємства, їхній вплив на конкурентоспроможність бізнесу, забезпечення безпеки персоналу та розвиток самої системи безпеки фірми ще достатньо не досліджені. Проте проблема інформаційної безпеки підприємства залишається недостатньо дослідженою. Це пов'язано з тим, що автори значну увагу приділяють забезпеченню інформаційної безпеки держави, а також з відсутністю цілеспрямованого підходу до проблеми в цілому у тих учених, які розглядали роль інформації в діяльності підприємства.

Метою нашої статті є вивчення основних вимог щодо забезпечення інформаційної безпеки підприємства, в розробці основних заходів щодо попередження виникнення загроз втрати та знищення інформації.

Усі економічно розвинуті країни світу використовують переваги інформаційних технологій у виробничій, комерційній та банківських сферах. Це пояснюється тим, що традиційні методи не дозволяють зорієнтуватись в сучасному інформаційному потоці і проаналізувати динамічні процеси економічної діяльності підприємства. Швидше за все розвиваються технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд та ін. [3, с. 32]. Зі зростанням науково-технічного прогресу зростає і необхідність вирішення проблеми інформаційної безпеки. Інформація – це чинник, який може призвести до технологічних аварій, військових та політичних конфліктів, дезорганізації державного управління, фінансової системи. Необхідно зазначити, що в науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека підприємства», що є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій і супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору. Так, Б. Кормич трактує інформаційну безпеку як стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин .

Деякі вчені розглядають інформаційну безпеку як стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [3, с. 72]. Інформаційну безпеку суспільства також визначають як неможливість заподіяння шкоди його духовній сфері. Економічні науки культурним цінностям, соціальним регуляторам поведінки людей, інформаційній інфраструктурі й повідомленням, що передаються за її допомогою [8, с. 64]. Із розвитком інформатизації, яка спостерігається останніми роками, з'явилась ще одна глобальна проблема – інформаційна безпека. Більша частина інтересів підприємства визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні дії з боку зовнішніх або внутрішніх джерел можуть задавати шкоду цим інтересам і становлять реальну загрозу для подальшої діяльності підприємства. Не викликає сумніву і той факт, що між рівнем економічної безпеки і інформаційною складовою існує пряма залежність. Як показує практика, будь-яка акція, спрямована проти господарюючого суб'єкта, розпочинається зі збору інформації, саме тому питання інформаційної безпеки давно ввійшли до головних пріоритетів практично всіх великих підприємств. Усе більше керівників розуміють, наскільки небезпечною може бути інсайдерська інформація, системи обробки інформації і дії співробітників, які беруть участь у діяльності підприємства [9].

Для регулювання економічної безпеки на підприємстві створюється служба інформаційної безпеки, що має виявляти і наочно демонструвати власникам підприємства весь спектр загроз в інформаційній сфері. Завдання керівників служби переконати, що протистояти загрозам можна тільки на основі створення і упровадження ефективних систем захисту інформації [2]. Виділимо найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо [8, 10].

Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту. Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки. У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями [9]:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз . Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті.

Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання. Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз.

Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування − способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу.

Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

Регламентація − найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус − методи захисту інформації, тісно пов’язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені виконувати встановлені правила.

Коли використовуються способи впливу на працівників, за яких вони виконують інструкції з етичних і особистісним міркувань, то йдеться про спонукання . Способи захисту інформації передбачають використання певного набору засобів.

Для запобігання втрати та витоку таємних даних використовуються засоби:

– фізичні;

– апаратні;

– програмні;

– апаратно-програмні;

– законодавчі;

– криптографічні та організаційні методи.

Фізичні засоби захисту − це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об’єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Апаратні засоби захисту − це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв’язку тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту − це засоби, які основані на синтезі програмних та апаратних засобів.

Законодавчі засоби − комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації. Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу .

Отже, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. В свою чергу, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

Список використаної літератури

1. Гуцу С. Ф. Правові основи інформаційної діяльності : навч. посіб. / С. Ф. Гуцу. – Х. : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. — 48 с.
2. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. – Х., 2004. – 42 с.
3. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. – 2011. – № 21. – С. 92–95.
4. Сороківська О. А. Інформаційна безпека підприємства : нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2. – Т. 2. – С. 32–35.
5. Кулініч О. А. Структурні чинники економічної безпеки України / О. А. Кулініч // Шлях України до економічної безпеки : матеріали наук.-практ. конф. – Х. : ХНУВС, 2007. – С. 59–63.
6. Живко З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. І. Керницька. – Львів : Ліга-Прес, 2008. – 345 с.
7. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия / С. В. Кавун // Управління розвитком. – Х. : ХНЕУ, 2008. – Вип. 6. – С. 17–21.
8. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Марунич // Управління розвитком. – 2014. – № 14. – С. 130–132.
9. Иванов О. В. Информационная составляющая современных войн / О. В. Иванов // Вестн. Моск. ун-та: сер. 18 : Социология и политология. – 2004. – № 4. – С. 64–70.
10. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. – М. : Гелиос АРВ, 2007. — 256 с.