Захаров О.І. – заступник директора
ННІ менеджменту безпеки
Університету економки та права „КРОК”, к.е.н., доцент

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті розглянуті теоретичні питання пов'язані з організацією діяльності по забезпеченню інформаційної безпеки підприємства в умовах інформаційної економіки. Розглянуто основні завдання й принципи діяльності системи забезпечення інформаційної безпеки. Запропоновано модель комплексного інформаційного забезпечення системи економічної безпеки підприємства.

Oleksandr Zaharov
PhD in Economics, Associate Professor
Deputy Director of Security Management Institute (KROK University)

INFORMATIVE PROVIDING OF MANAGEMENT BY SYSTEM OF ECONOMIC SECURITY OF ENTERPRISE

In the article theoretical questions related to organization of activity on providing of informative security of enterprise in the conditions of informative economy are considered. Basic tasks and principles of activity of the system of providing of informative security are considered. The model of the complex informative providing of the system of economic security of enterprise is offered.

Постановка проблеми

В сучасних умовах на економічну безпеку підприємств вагомий вплив має її інформаційна складова. Це обумовлено тим, що саме через інформаційне середовище здійснюються багато загроз та ризиків у різних сферах економічної діяльності.

Останнім часом усе частіше висловлюється думка про те, що в третім тисячоріччі лідерство у світі буде визначатися спроможністю держав контролювати інформаційні процеси. Це обумовлено тим, що в даний час активно відбувається перехід від

економічної до інформаційної ери розвитку цивілізації. Інформація розглядається як сукупність знань про фактичні дані і залежність між ними і є найбільш високоліквідним товаром. Вартість інформації і її своєчасної доставки в потрібне місце постійно зростає.

Інтенсивний розвиток інформаційних технологій сприяє більш ефективному й економічному використанню матеріальних і людських ресурсів. І тому не випадково найбільш економічно розвинені країни щороку збільшують фінансування цих технологій.

Інформація сьогодні проникає в усі сфери економічної діяльності, здобуває конкретне матеріальне і вартісне вираження. Перебудова суспільства на нових інформаційних основах обумовила потребу визначення нових підходів до вирішення проблем інформаційного забезпечення системи економічної безпеки підприємства в інформаційної економіки.

Аналіз останніх досліджень і публікацій

Проблема комплексного забезпечення інформаційної безпеки досить широко розглянута в працях ряду вітчизняних і закордонних авторів. Великий внесок у розробку теоретичних основ інформаційної безпеки внесли вчені й фахівці в цій області - Архипов А., Гаценко О., Жуків А., Маркин И., Конеев И., Бєляєв А., Ярочкин В.И. та інші.

Однак всі дослідження з даної проблеми носять як правило однобічний характер. Автори [4, 5, 9, 10] розглядають дану проблему в основному тільки з позиції захисту інформації від несанкціонованого доступу. Це, безумовно, важливий напрямок забезпечення інформаційної безпеки, але не вирішальну проблему в цілому. Автори на наш погляд недостатню увагу приділяють іншому не менш важливому напрямку інформаційної безпеки пов'язаному із забезпеченням підприємства достовірною інформацією про процеси що відбуваються на ринку, конкурентах, інноваціях і т.д. мають життєво важливе значення для стабільної роботи й розвитку підприємства, а також забезпечення його економічної безпеки.

Сьогодні потрібні нові підходи до побудови системи комплексного забезпечення інформаційної безпеки як важливою складової економічної безпеки підприємств. В основі яких повинен бути не тільки захист інформаційних ресурсів підприємства. Важливо також своєчасно забезпечити керівництво підприємства достовірною інформацією щодо процесів яки відбиваються в зовнішньому і внутрішньому середовище.

В умовах кризи світової й вітчизняної економік, коли підприємствам доводиться зіштовхуватися з перманентними небезпеками, загрозами й ризиками доцільно переглянути існуючі підходи до інформаційного забезпечення системи економічної

безпеки підприємств. На наш погляд система інформаційної безпеки підприємств повинна бути комплексною.

Невирішені частини проблеми

Сучасним підприємствам доводиться працювати в умовах інформаційної економіки. У цих умовах найважливішим завданням власників і керівників підприємства і його системи безпеки є рішення проблеми пов'язаної з розробкою ефективної політики й стратегії інформаційної безпеки, а також вибором ефективних технологій, форм і методів забезпечення інформаційної безпеки. Рішення цієї проблеми значною мірою ускладнене тим, що в цей час темпи розвитку інформаційних технологій значно випереджають темпи розробки рекомендаційної й нормативно-правової бази керівних документів, що діють на території України. У цей час відсутні основні документи, що регламентують всю діяльність по забезпеченню інформаційної безпеки підприємства. Внаслідок цього, на додаток до вимог і рекомендацій стандартів, Конституції, законам і іншим керівним документам необхідно використати ряд міжнародних рекомендацій. У тому числі адаптувати до вітчизняних умов і застосовувати на практиці методики міжнародних стандартів, таких, як ISO 17799, ISO 9001, ISO 15408 і інші, а також використати методики керування інформаційними ризиками в сукупності з оцінками економічної ефективності інвестицій у систему забезпечення захисту інформаційних ресурсів і інтелектуальної владності на підприємстві.

Метою статті є розробка моделі комплексного забезпечення інформаційної безпеки підприємства, визначення її цілей, завдань та принципів діяльності.

Виклад основного матеріалу

В умовах інформаційної економіки успішна діяльність у вирішальному ступені залежить від своєчасного одержання інформації про процеси що відбуваються на ринку, конкурентах, сучасних технологіях і інноваціях, а також від рівня надійності захисту своїх інформаційних ресурсів і інтелектуальної владності.

Інформаційна безпека - це такий стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через

несанкціоноване поширення інформації. Інформаційна безпека з погляду економічних інтересів нині має особливу актуальність і розглядається як одна з пріоритетних задач стратегічного керування. Інформаційний простір і його інформаційне наповнення варто віднести до найважливіших ресурсів підприємства, здатних приносити великий дохід.

Ефективне інформаційне забезпечення є найважливішою умовою реалізації концепції економічної безпеки та забезпечення ефективного стратегічного управління підприємством. Один з підходів до побудови системи забезпечення інформаційної безпеки підприємства наданий на рис. 1.

Рис. 1. Загальна схема забезпечення інформаційної безпеки підприємства

Обґрунтування стратегічних рішень щодо забезпечення економічної безпеки підприємства, від яких залежить його стабільне функціонування і розвиток базується на достовірної інформації про стан внутрішнього та зовнішнього середовища. При цьому інформація повинна носити системний характер. Одна з задач інформаційної безпеки підприємства полягає в запобіганні використання його інформаційного середовища для поширення помилкової або невірної інформації про процеси, що відбуваються в зовнішнім середовищі, а також для збору стратегічно важливої для конкурентів інформації про його внутрішнє середовище.

Разом з тим, слід враховувати, що інформаційна загроза, у силу системності всієї сукупності загроз, підсилює небезпеку внутрішніх і зовнішніх загроз. Це обумовлено тим, що більшість факторів, що впливають на прийняття рішень на всіх етапах розробки і реалізації стратегій, носить інформаційний характер. Тому ефективне інформаційно-аналітичне забезпечення господарської діяльності підприємства передбачає проведення всебічного аналізу й обробки всієї повноти одержуваних даних як у розрізі питань компетенції окремих функціональних підрозділів підприємства, так і в розрізі проблем, що стосуються загально корпоративної політики.

В силу складності аналітичного процесу особливу важливість здобувають питання координації взаємодії різних підрозділів підприємства в процесі проведення робіт з аналізу й обробки інформації. Система економічної безпеки підприємства повинна розпізнавати інформаційний вплив, аналізувати отриману інформацію і, з метою захисту, формувати в системі управління відповідну реакцію на дії зовнішнього середовища. Для успішного рішення цієї задачі необхідно організувати ефективну роботу зі збору усіх видів інформації, що має відношення до діяльності даного підприємства. До інформації такого роду можна віднести :

- Інформацію про сучасний і можливий стан ринків, на яких працює підприємство.
- Інформацію про тенденцію макроекономічного розвитку світової і національної економік.
- Науково-технічну інформацію, що стосується сфер діяльності підприємства.
- Джерелами інформації, збір і аналіз якої необхідні для забезпечення інформаційної безпеки підприємства, можуть бути:
- Різні офіційні джерела (офіційні видання, звіти і документи державних чи інших органів і організацій), що містять відкриту офіційну інформацію.
- Неофіційні джерела, що містять більш-менш достовірну усну чи іншу нетаємну інформацію, одержувану з неформальних контактів з носіями даної інформації.
- Конфіденційна інформація, одержувана співробітниками підприємства шляхом

несанкціонованого доступу до цієї інформації.

- Внутрішня інформація, що стосується всіх аспектів діяльності даного підприємства.
- Для одержання вище зазначеної інформації можуть застосовуватися різні методи в тому числі:
- Вивчення різних відкритих інформаційних видань.
- Співробітництво з метою одержання інформації з інформаційними агентствами.
- Використання мережі INTERNET.
- Офіційні зв'язки з органами державного керування всіх рівнів.
- Використання бази даних наукових організацій, фондів, бібліотек, архівів.
- Одержання відкритої і закритої інформації за допомогою контактів співробітників підприємства з представниками різних державних і комерційних організацій і інших компетентних осіб;
- Організація системи збору й аналізу усередині корпоративної інформації з усіх аспектів діяльності підприємства.
- Методи проведення аналізу інформації з діяльності підприємства можна розділити на групу локальних методів і групу методів загально корпоративного аналізу.

До першої групи відносяться методи, що застосовуються для аналізу специфічних проблем відносно якогось функціонального підрозділу підприємства, а до другої - такі аналітичні методи:

- Порівняльний аналіз.
- Логічний аналіз причинно-наслідкових взаємозв'язків подій і процесів.
- Статистичні методи аналізу.
- Різні види моделювання процесів і ситуацій.
- Аналіз проектів.
- Основними принципами організації роботи з аналізу одержуваної інформації є:
- Систематизація і класифікація одержуваної інформації.
- Постійна і безупинна аналітична діяльність.
- Усебічний характер аналітичних процесів на підприємстві.

Дуже важливо правильно класифікувати всю одержувану інформацію за ступенями важливості для забезпечення економічної безпеки підприємства. Для цього пропонується система класифікація інформації в основу якої покладені чотири рівні важливості.

1. Життєво важлива - незамінна інформація, наявність якої необхідно для функціонування підприємства. Витік цієї інформації ставить під загрозу саме функціонування організації (підприємства).

2. Важлива - інформація, процес ліквідації наслідків витоку якої завдає матеріальної шкоди підприємству, однак воно може ефективно функціонувати й у випадку витоку інформації.

3. Корисна - інформація, витік якої завдає матеріальної шкоди підприємству і не впливає на його функціонування.

4. Несуттєва - інформація, витік якої не завдає матеріальних збитків підприємству і не впливає на його функціонування.

Інформація, що відноситься до перших, трьох рівнів, є комерційною таємницею.

Таким чином інформаційна безпека займає особливе місце в системі стратегічного керування. Це пов’язано з тим, що інформаційні відносини і процеси пронизують усі відносини що мають місце у суспільстві і економіці. В наступний час система зовнішніх і внутрішніх загроз інформаційної безпеки підприємства має комплексний, всеохоплюючий для всіх сфер його діяльності характер. В сучасних умовах при широкому використанні різноманітних інформаційних технологій, питання інформаційної безпеки підприємств набувають великого значення для забезпечення економічної безпеки підприємств.

Для надійного забезпечення інформаційної безпеки підприємства необхідно вирішити ряд досить складних завдань пов'язаних з перспективним стратегічним розвитком підприємства. Необхідна ефективна політика й стратегія інформаційної безпеки, які повинні враховувати перспективи розвитку підприємства, що також течуть і перспективні небезпеки, погрози й ризики.

Для цього необхідно. По-перше, кількісно оцінити поточний рівень інформаційної безпеки підприємства, що зажадає виявлення ризиків на правовому, організаційно-управлінському, технологічному, а також технічному рівнях забезпечення захисту інформації. По-друге, розробити політику, стратегію й тактичні плани вдосконалювання корпоративної системи захисту інформації для досягнення прийнятного рівня захищеності інформаційних ресурсів підприємства. Для цього необхідно:

- обґрунтувати й зробити розрахунок фінансових вкладень у забезпечення безпеки на основі технологій аналізу ризиків, співвіднести витрати на забезпечення безпеки з потенційним збитком і ймовірністю його виникнення;
- виявити й провести першочергове блокування найнебезпечніших напрямків до здійснення атак на ресурси підприємства;

- визначити функціональні відносини й зони відповідальності при взаємодії підрозділів і осіб по забезпеченню інформаційної безпеки підприємства, створити необхідний пакет організаційно-розпорядницької документації;
- розробити й погодити зі службами організації, наглядовими органами проект впровадження необхідних комплексів захисту, що враховує сучасний рівень і тенденції розвитку інформаційних технологій;
- забезпечити підтримка впровадженого комплексу захисту відповідно до умов роботи підприємства що змінюються, регулярними доробками організаційно-розпорядницької документації, модифікацією технологічних процесів і модернізацією технічних засобів захисту.

Основними цілями забезпечення інформаційної безпеки підприємства є:

- пошук і одержання інформації необхідної для забезпечення стабільної діяльності й динамічного розвитку підприємства і його систем безпеки в умовах перманентних небезпек, погроз і ризиків ринкової економіки;
- виключення використання недостовірної інформації в системі керування підприємством, у його виробничій діяльності й у системі безпеки;
- запобігання несанкціонованого доступу до інформаційних ресурсів підприємства;
- запобігання витоку, розкрадання й втрати інформації на підприємстві;
- запобігання перекручування й підробки інформації застосовуваної в системі керування, виробничої діяльності й у системі безпеки підприємства;
- запобігання несанкціонованих дій по знищенню, модифікації, перекручуванню, копіюванню, блокуванню інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси й інформаційні системи підприємства;
- захист інтелектуальної владності на підприємстві.

З огляду на, що в остаточному підсумку головної ціль будь-якої системи безпеки є забезпечення стійкого функціонування й розвитку підприємстві. Необхідно при забезпеченні інформаційної безпеки основна увага постійно приділяти на рішення наступних завдань:

- забезпечення власників (керівників) підприємства необхідної інформації для прийняття рішень на стратегічному й тактичному рівнях керування;
- своєчасне виявлення небезпек, погроз і ризиків для діяльності підприємства;
- запобіганні небезпек, погроз і неприйнятних ризиків для діяльності підприємства;

- захист інформації й інтелектуальної владності від протиправних зазіхань; інформаційне забезпеченні ефективної виробничої діяльності всіх структурних підрозділів підприємства і його систем безпеки.
- віднести інформацію до категорії обмеженого доступу (службовій таємниці);
- прогнозувати й вчасно виявляти погрози безпеки інформаційним ресурсам і інтелектуальній владності;
- вчасно виявляти причини й умови, що сприяють нанесенню фінансового, матеріального й морального збитку підприємству, порушенню його нормального функціонування й розвитку;
- створити умови функціонування з найменшою ймовірністю реалізації погроз безпеки інформаційним ресурсам і нанесення різних видів збитку;
- створити механізми й умови оперативного реагування на погрози інформаційної безпеки й прояву негативних тенденцій у їхньому функціонуванні;
- забезпечувати ефективне припинення зазіхань на інформаційні ресурси й інтелектуальну владність на основі правових, організаційних і технічних мір і засобів забезпечення безпеки;
- створити умови для максимально можливого відшкодування й локалізації збитку інформаційним ресурсам підприємства, що наноситься неправомірними діями фізичних і юридичних осіб, і тим самим послабити можливий негативний вплив наслідків порушення інформаційної безпеки.

Досягнення цілей і завдань забезпечення інформаційної безпеки підприємства повинне здійснюватися на основі дотримання наступних принципів:

- законності;
- комплексності;
- централізованого керування;
- координації й взаємодії із правоохоронними органами;
- самостійності й відповідальності за забезпечення безпеки;
- відповідність зовнішнім і внутрішнім погрозам безпеки підприємства;
- сучасної матеріально-технічної оснащеності;
- компетенції;
- конфіденційності;
- комплексного використання сил і засобів забезпечення інформаційної безпеки.

Для рішення завдань по забезпеченню інформаційної безпеки підприємства на наш погляд доцільно використати модель комплексного інформаційного забезпечення системи економічної безпеки підприємства, що надана на рисунку 2.

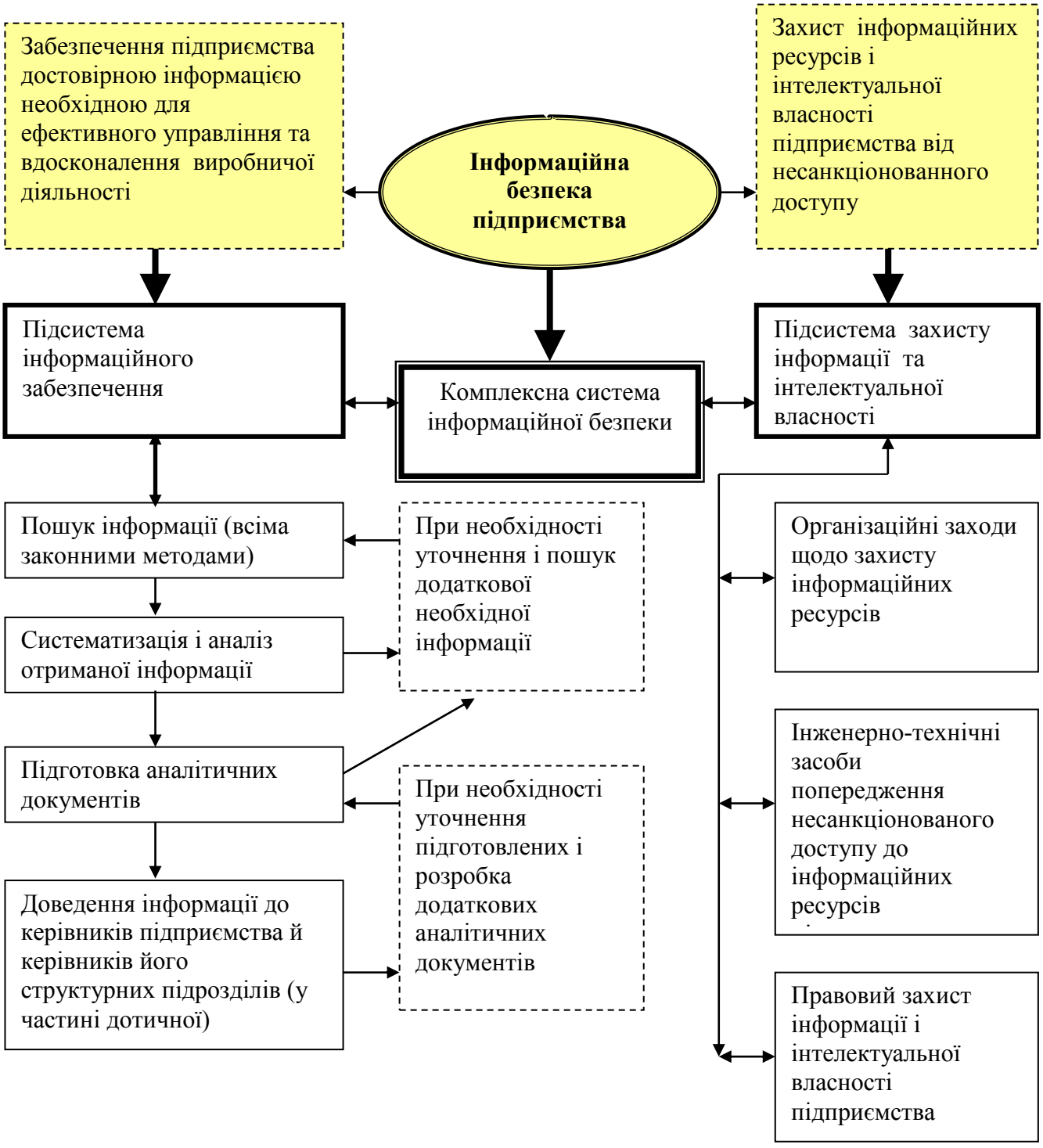

Рис. 2 Модель комплексного інформаційного забезпечення системи економічної безпеки підприємства

Запропонована модель системи забезпечення інформаційної безпеки підприємства складається із двох підсистем.

Перша підсистема інформаційного забезпечення. Дана підсистема призначена для своєчасного одержання в необхідних обсягах достовірної інформації, про процеси що

відбуваються на ринку, які можуть вплинути або впливають на діяльність і розвиток підприємства, а також стан його безпеки. Необхідна також інформація про конкурентну ситуацію, нові ідеї й наукові розробки, появі перспективних зразків техніки й технологій, інноваційних процесах і т.д. Без цієї інформації керівництво підприємства не може розробити ефективну стратегію, що відповідає реаліям ринку, а також здійснювати ефективне тактичне й оперативне керування й забезпечувати безпека. У запропонованій моделі визначено, щоб одержати необхідну інформацію для прийняття рішень у сфері керування підприємством необхідно здійснити всіма законними методами пошук потрібної інформації, потім провести систематизацію й аналіз отриманих відомостей, підготувати аналітичні документи й довести їх до керівництва підприємства й інших посадових осіб у частині дотичної.

При цьому постійно обновляти й поглиблювати інформацію з обліком поточних і перспективних напрямків діяльності підприємства і його систем безпеки. Особлива увага звертається на встановлення тісного взаємозв'язку між всіма елементами підсистеми інформаційного забезпечення системи інформаційної безпеки підприємства.

Друга підсистема призначена для захисту інформації й інтелектуальної власності підприємства. Вона включає організаційні заходи щодо захисту інформаційних ресурсів, інженерно-технічні засоби попередження несанкціонованого доступу до інформаційних ресурсів підприємства й правова захист інформації й інтелектуальної власності підприємства. Обидві підсистеми взаємозалежні між собою й працюють у єдиному алгоритмі.

На основі запропонованої моделі можна вирішити завдання комплексного забезпечення інформаційної безпеки підприємства.

Висновки

В умовах світової фінансово-економічної кризи успішна діяльність, безпека й розвиток підприємства в значній мірі залежить від стану його інформаційної безпеки. Протидіяти небезпекам, погрозам і ризикам для інформаційних ресурсів підприємства й забезпечити його безпека й стійкий розвиток можна тільки на основі комплексного підходу. Тільки комплексна система забезпечення інформаційної безпеки здатна в сучасних умовах вчасно виявляти, оцінювати й ефективно протидіяти небезпекам, погрозам і ризикам, інформаційним ресурсам підприємства, захищати його інтелектуальну

власності й вчасно забезпечувати керівництво необхідною достовірною інформацією про процеси що відбуваються у різних сферах внутрішнього й зовнішнього середовища.

Основою комплексної системи безпеки є корпоративні ресурси підприємства, а також ресурси різних зовнішніх організацій, з якими здійснюється взаємодія на основі взаємного інтересу по протидії небезпекам, погрозам і ризикам діяльності підприємства.

Запропонована модель системи комплексного забезпечення інформаційної безпеки підприємства дозволяє побудувати ефективну систему захисту інформаційних ресурсів підприємства і його інтелектуальної власності, а також забезпечити інформацією необхідної для розробки стратегій і тактичних планів і забезпечення ефективного керування в умови високої невизначеності зовнішній середовища.

Список використаних джерел

1. Закон України "Про інформацію" від 02.10.1992р.
2. Закон України "Про державну таємницю" від 21.01.1994р.
3. Постанова КМУ №611 "Про перелік документів, що не становлять комерційної таємниці" від 09.08.1993 р.
4. Архипов А. В. Информационная защита объекта - задача многогранная. - М., 2001. - 220 с.
5. Гаценко О.Ю. Защита информации. Основы организационного управления. - Спб., 2001, - 228 с.
6. Домарев В.В. Защита информации и безопасность компьютерных систем. - К., 1999, - 192 с.
7. Драга А.А. Комплексное обеспечение безопасности фирмы. - М., 2001, - 265 с.
8. Драчев С.С. Основы корпоративной безопасности. - Спб., 2000, - 240с.
9. Жуков А.В., Маркин И.Н., Денисов В.Б. Все про защиту коммерческой информации. - М., 2000, - 232 с.
10. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - Спб., 2003, - 752 с.
11. Ярочкин В.И. Информационная безопасность: учебное пособие. - М., 2000, - 400 с.