УДК 330.75:658.15

Олександра В. Ольшанська, Наталія В. Раллє
Київський національний університет технологій та дизайну

СУТНІСТЬ ТА СУЧАСНІ ПРИНЦИПИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

У статті розглянуто підходи до трактування сутності інформаційної безпеки підприємства та її значення в системі управління підприємством, розкриті методи та способи інформаційної безпеки, запропоновані сучасні принципи використання інформаційної безпеки на підприємстві.

Ключові слова: *інформаційна безпека, інформаційна система, інформаційні технології, загрози інформаційної безпеки, криптографія, програмно-технічне забезпечення, стенографія.*

Александра В. Ольшанская, Наталия В. Ралле
Киевский национальный университет технологий и дизайна

СУЩНОСТЬ И СОВРЕМЕННЫЕ ПРИНЦИПЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В статье рассмотрены подходы к трактовке сущности информационной безопасности предприятия и ее значение в системе управления предприятием, раскрыты методы и способы информационной безопасности, предлагаемые современные принципы использования информационной безопасности на предприятии.

Ключевые слова: *информационная безопасность, информационная система, информационные технологии, угрозы информационной безопасности, криптография, программно-техническое обеспечение, стенография.*

Oleksandra V. Ol'shanska, Nataliia V. Rallie
Kiev National University of Technologies and Design

ESSENCE AND MODERN PRINCIPLES OF THE USE OF INFORMATION SECURITY FOR THE ENTERPRISE

The article describes the approaches to the interpretation of the essence of the enterprise information security and its importance in the enterprise management system, described methods and techniques of information security, suggested use of modern principles of information security in the enterprise.

Keywords: *information security, information systems, information technology, information security threats, cryptography, software and technical support, stenography.*

Постановка проблеми та її зв'язок з важливими науковими та практичними завданнями. Одним із пріоритетних напрямків державної політики є розвиток інформаційного суспільства та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя.

Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників. В умовах економіки постіндустріального суспільства, інформація стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки – усе більш складними і практично значущими. Інформаційна безпека є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства.

Аналіз останніх публікацій по проблемі. Питанням інформаційної безпеки присвячено увагу у працях таких науковців як: В. Цимбалюк [2], В. Фурашев [3], С. Гуцу [4], О. Литвиненко [5], О. Сороківська [6], М. Танцюра [7] та інших. Вітчизняними науковцями було сформульовано основні цілі інформаційної безпеки та напрями забезпечення

інформаційної безпеки. Охарактеризовано економічну необхідність забезпечення інформаційної безпеки.

Невирішені частини дослідження. Питанням інформаційної безпеки присвячено багато праць сучасних науковців, проте проблеми забезпечення інформаційної безпеки підприємства потребують постійного удосконалення у зв'язку із розвитком сфери інформаційних технологій. впровадження інновацій та захист інформації, адже динамічний розвиток наукоємних секторів та їх інформаційна безпека прямо впливає на рівень розвитку економіки в цілому.

Постановка завдання. Таким чином, ці проблеми, будучи актуальними завжди, придбали особливу та вимагають особливої уваги до інформаційної безпеки. Все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим обсягом інформації, вдосконаленням засобів її зберігання, передачі та обробки. Особливістю сьогодення є стрімкий розвиток та повсюдне використання інформаційних технологій, завдяки чому інформація стає найважливішим продуктом як на виробництвах, в державних установах, так і в повсякденному житті громадян. Тому одним з пріоритетних питань стає забезпечення інформаційної безпеки на різних рівнях.

Мета дослідження. Метою статті є визначення сутності інформаційної безпеки та розроблення принципів її використання на підприємстві.

Виклад основних результатів та їх обґрунтування. Наявність значної частини інформації в електронній формі, використання локальних і глобальних мереж створюють якісно нові загрози конфіденційної інформації. Наукова література не визначає єдиного погляду на зміст поняття «інформаційна безпека» та «інформаційна безпека підприємства».

Визначення різними авторами поняття інформаційної безпеки наведене у таблиці 1.

Таблиця 1

Визначення поняття інформаційної безпеки

Автор	Визначення поняття інформаційна безпека
В. Цимбалюк	стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [2].
В. Фурашев	вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [3].
С. Гуцу	стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [4].
О. Литвиненко	єдність трьох складових: забезпечення захисту інформації, захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [5].

Сороківська О.А. визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [6].

М. Танцюра характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації. Доступність - це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність - це властивість захищеності точності та повноти даних; конфіденційність - це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи - це знання чи дані, які мають цінність для організації [7].

А. Марущак тлумачить інформаційну безпеку підприємства – як цілеспрямовану діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [8].

Таким чином можна стверджувати, що пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

У більш загальному випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [9].

Захист інформації – це процес, спрямований на забезпечення інформаційної безпеки. Визначальними факторами інформаційної безпеки є загроза і ризик. Загрозою називають потенційну причину (подія, порушення, інцидент), що знижує рівень інформаційної безпеки системи, тобто потенційно здатну привести до негативних наслідків і збитку системи або організації.

Ризик являє собою можливий збиток, тобто комбінацію (як правило, твір) ймовірності реалізації загрози і шкоди від неї. Відзначимо, що загроза і ризик визначаються не взагалі, а щодо конкретного об'єкта ресурсу, що захищається . У термінології менеджменту бізнес-процесів замість ресурсу використовується синонімічне поняття - актив, під визначення якого підпадає все, що має цінність для організації.

Прикладами таких активів є: інформація, програмне забезпечення, апаратне забезпечення, інформаційна система (складний актив, що включає попередні), людина, імідж організації. У підсумку, активами представляються всі ті об'єкти, які підлягають захисту шляхом вибудовування процесів інформаційної безпеки.

Загрози класифікують по ряду критеріїв:

– з причини виникнення (природні або техногенні, в тому числі навмисні або випадкові);

– по розташуванню джерела (зовнішні або внутрішні);

– по компрометованій підсистемі або сегменту (мережеві, криптографічні та ін.);

– по етапу формування в життєвому циклі системи (реалізаційні і експлуатаційні);

– за результуючою дією (порушують цілісність, конфіденційність, доступність).

В залежності від виду загроз інформаційній безпеці останню можна розглядати наступним чином:

– як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;

– як забезпечення стану захищеності інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

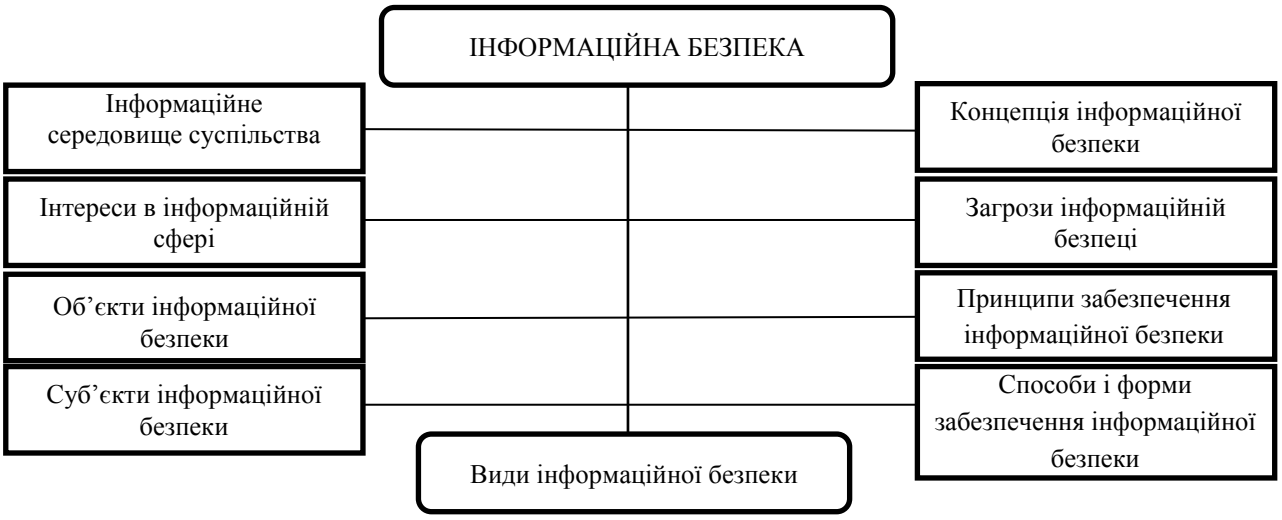
– як забезпечення стану захищеності інформаційних прав і свобод людини і громадянина.

Основні поняття інформаційної безпеки наведені на рисунку 1.

Об'єктами інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційні системи різного масштабу і різного призначення.

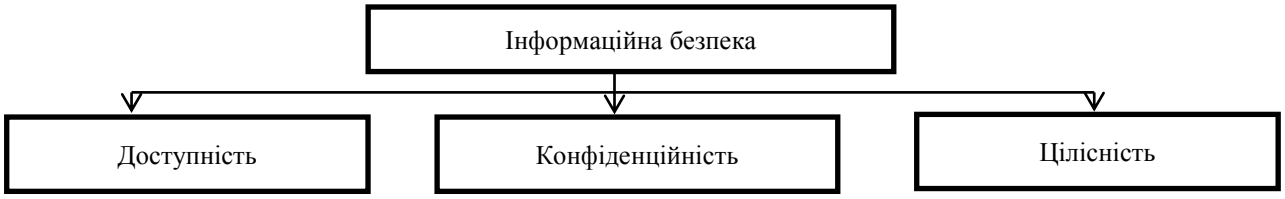
До суб'єктів інформаційної безпеки відносяться: держава, що здійснює свої функції через відповідні органи; громадяни суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства.

Спектр інтересів суб'єктів, зв'язаних з використанням інформаційних систем, можна розділити на наступні категорії (рис. 2): забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів та інфраструктури, що її підтримує.



Джерело: [10]

Рис. 1. Основні поняття інформаційної безпеки



Джерело: [11]

Рис. 2. Базові критерії інформаційної безпеки

Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо за тими або іншими причинам надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Основна роль доступності виявляється в різного роду системах управління - виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки - і матеріальні, і моральні може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних га авіаквитків, банківські послуги тощо).

Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Конфіденційність - найбільш опрацьований аспект інформаційної безпеки. На жаль, практична реалізація заходів по забезпеченню конфіденційності сучасних інформаційних систем характеризується певними труднощами. По-перше технічні канали просочування інформації є закритими, так що більшість користувачів позбавлене можливості скласти уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми.

До основних задач забезпечення інформаційної безпеки належать:

– виявлення, оцінка та прогнозування джерел загроз інформаційній безпеці,

– розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації,

– створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ та підприємств по реалізації політики інформаційної безпеки;

– розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідації наслідків її порушення,

– забезпечення участі України в процесах створення і використання глобальних інформаційних мереж та систем [12].

Захист інформації, забезпечення інформаційної безпеки повинно носити системний характер, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні) повинні застосовуватися одночасно і під єдиним управлінням. Існує велика кількість інструментів забезпечення інформаційної безпеки засоби ідентифікації та автентифікації користувачів; засоби шифрування інформації, міжмережні екрани; віртуальні приватні мережі; засоби контентної фільтрації; інструменти перевірки цілісності вмісту дисків; засоби антивірусного захисту, системи виявлення уразливостей мереж і аналізатори мережних атак. Особливе місце займають криптографічні методи для захисту інформації. Інтерес комерційних структур до них значно зріс у зв'язку зі зменшенням вартості перехоплення інформації, що передається електронною поштою чи функціонує в системі електронних платежів. Найпоширенішими вважаються методи кодування та шифрування інформації. Поряд з ними використовуються методи розділення та стиснення даних. У процесі захисту передачі усної інформації використовують методи аналогового скемблірування та дискретизації мови з подальшим шифруванням.

Один із перспективних напрямів захисту інформації є розроблення методів стенографії, що базуються на різних принципах, забезпечують таємницю самого факту існування секретної інформації в тому чи іншому середовищі за допомогою відповідних засобів: невидимих чорнил, мікрофотознімків, таємних каналів та засобів зв'язку з плаваючими частотами тощо. Незважаючи на використання зазначених методів, забезпечення інформаційної безпеки підприємства на належному рівні можливе лише тоді, коли інформаційна складова економічної безпеки розглядатиметься як невід'ємний елемент процесу управління підприємством.

Досвід показує, що практично кожне підприємство має антивірусні засоби захисту, системи ідентифікації користувачів, системи управління доступом до інформаційної системи тощо. Тобто потенціал засобів захисту є, але він не реалізується фірмами повністю. Більш того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть наполовину не використовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту [13].

Таким чином, комплексне забезпечення інформаційної безпеки автоматизованих систем - це сукупність криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації при її обробці, зберіганні та передачі з використанням сучасних комп’ютерних технологій [14].

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб [15].

Важливим є визначення етапів побудови політики інформаційної безпеки, а саме:

– реєстрація всіх ресурсів, які мають бути захищені;

– аналіз та створення переліку можливих загроз для кожного ресурсу;

– оцінка ймовірності появи кожної загрози;

– вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему [16].

На практиці інформаційна безпека включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку.

Структура системи залежить від об'єму та цінності інформації, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи. Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо всі інформаційні ресурси системи дотримуються відповідного рівня конфіденційності, цілісності (неможливості навмисної або випадкової її модифікації) і доступності.

Можна виділити такі підсистеми ефективного захисту інформації на підприємстві

– Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.

– Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.

– Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.

– Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.

– Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.

– Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.

– Підсистема захисту систем управління базами даних.

– Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.

– Підсистема захисту мобільних пристроїв.

– Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них [11].

Висновки та перспективи подальших досліджень. В економічній сфері забезпечення захисту інформаційних ресурсів та комунікативних каналів від конкурентної розвідки є передумовою успішності будь-якого бізнесу; підтримка вітчизняних виробників високотехнологічної продукції, формування вітчизняної індустрії інформаційних послуг, комплексна інформатизація виробничих процесів сприяє розвитку промисловості; дотримання вимог інформаційної безпеки в системах збирання, обробки, зберігання і передачі статистичної, фінансової, біржової, податкової та митної інформації забезпечує конкурентні переваги.

Проблема інформаційної безпеки має особливе значення в умовах, коли в суспільстві зрозуміли, що інформаційні ресурси є об'єктом власності і мають товарну цінність. Вона не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації.

References

1. DOPOVID «Pro stan informatyzatsii ta

Література

1. ДОПОВІДЬ «Про стан інформатизації

rozvytok informatsiinoho suspilstva v Ukraini za2012 rik». [Elektronnyi resurs].– Rezhym dostupu: http://dknii.gov.ua/sites/default/files/skachannye_fayly.pdf

2. Tsymbaliuk V.S. Okremi pytannia shchodo vyznachennia katehorii «informatsiina bezpeka»u normatyvno-pravovomu aspekti / V.S Tsymbaliuk // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini – 2004.№8 S.30–33

3. Furashev V.M. Pytannia zakonodavchoho vyznachennia poniatiinokatehoriinoho aparatu u sferi informatsiinoi bezpeky i V.M Furashev // Informatsiia i pravo: naukovyi zhurnal.K.: NDTsPI NAPrN Ukrainy, 2012. – № 1(4)S.46–56.

4. Hutsu S.F Pravovi osnovy informatsiinoi diialnosti: navchalnyi posibnyk / S.F. Kutsu. X.: Nats. aerokosm. un-t «Khark. aviats. in-t», 2009. – 48 s.

5. Lytvynenko O.V Problemy zabezpechennia informatsiinoi bezpeky v postradianskykh krainakh (na prykladi Ukrainy ta Rosii): avtoref. dys. na zdobuttia nauk, stupenia kand. polit nauk: spets. 23.00.04 / O V Lytvynenko. - K., 1997 – 18 s.

6. Sorokivska O.A , Hevko V.L Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy. [Elektronnyi resurs]. – Rezhym dostupu: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

7. Tatsiura M.Iu. Problemni aspekty standartyzatsii u haluzi informatsiinoi bezpeky pidpryiemstva // Materialy Druhoi nauk.-prakt. konf. «Stalyi rozvytok ta ekolohichna bezpeka suspilstva v ekonomichnykh transformatsiiakh» 23–24 veresnia 2010 r m, Bakhchysarai, NDI staloho rozvytku ta pryrodokorystuvannia, RVPS Ukrainy NAM Ukrainy, Krymskyi instytut KNEU im. Vadyma Hetmana / M.Iu. Tatsiura. – Simferopol Feniks, 2010 – S. 451-453.

8. Marushchak A. 1. Informatsiino-pravovi napriamy doslidzhennia problem informatsiinoi bezpeky /U Derzhavna bezpeka Ukrainy / A.1. Marushchak. – 2011. – № 21. – S. 92–95.

9. Lytvyniuk A.A. Osnovy informatsiinoi

та розвиток інформаційного суспільства в Україні за 2012 рік». [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/sites/default/files/skachannye_fayly.pdf

2. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека»у нормативно-правовому аспекті / В.С Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – 2004.№8 С.30–33

3. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки і В.М Фурашев //Інформація і право: науковий журнал.К.: НДЦПІ НАПрН України, 2012. – № 1(4)С.46–56.

4. Гуцу С.Ф Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Куцу. Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 48 с.

5. Литвиненко О.В Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук, ступеня канд. політ наук: спец. 23.00.04 / О В Литвиненко. – К., 1997 – 18 с

6. Сороківська О.А, Гевко В.Л Інформаційна безпека підприємства: нові загрози та перспективи.[Електроннийресурс]. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

7. Тацюра М.Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ. конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23–24 вересня 2010 р м, Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАМ України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М.Ю. Тацюра.– Сімферополь Фенікс, 2010 – С.451–453.

8. Марущак А. 1. Інформаційно-правові напрями дослідження проблем інформаційної безпеки /У Державна безпека України / А.І. Марущак. – 2011. – № 21. – С. 92–95.

9. Литвинюк А.А. Основи інформаційної

bezpeky. Kompleksna systema zakhystu informatsii: struktura, vstanovlennia ta pidtrymka funktsionuvannia// A.A. Lytvyniuk – [Elektronnyiresurs]. –Rezhym dostupu:http://www cvk.gov.ua/visnyk/pdf/2008 4/visnik st 08.pdf

10. Balashov P. A. Otsenka riskov informatsionnoy bezopasnosti na osnove nechetkoy logiki / P A. Balashov, V P. Bezguzikov, R.I. Kislov // [Elektronniy resurs] – Rezhim dostupu: http://www nwaktiv.ru/textstat2/index.htm1

11. Korchenko A.G. Metody analiza i otsenki riskov poter' gosudarstvennykh informatsionnykh resursov / Korchenko A.G., Shcherbina V.P., Kazmirchuk S.V. // Zashchita informatsii – 2012. – №1. – S. 126–139.

12. Batiuk A Ie Informatsiini systemy v menedzhmenti / A.Ie Batiuk, Z.P. Dvulit, K M. Obelovska, YiM Ohorod ni k, L.P. Fabri. – Lviv: «IntelektZakhid», 2004 –S 343–384.

13. Kazakevych O. Iu Predprynymatel v opasnosty: sposobы zashchytы Praktycheskoe rukovodstvo dlia predprynymatelei y byznesmenov / O Iu. Kazakevych, N V Konev. – M Yurfak MHU, 2011. - 152 s.

14. Ananskiy Є. V Zashchita informatsii-osnova bezopasnosti biznesa, zhurnal «Biznes i bezopasnost'«. – 2009. – S 18.

15. Brodska D. V. Otsinka produktyvnosti pidpryiemstva yak skladova systemy zabezpechennia yoho efektyvnoho funktsionuvannia / D V. Brodska [Elektronnyi resurs] – Rezhym dostupu: http://vestnikdnu sot ua/archive/201264/brodska.html

16. Ortynskyi V. L. Ekonomichna bezpeka pidpryiemstv, orhanizatsii ta ustanov i V. L. Ortynskyi [Elektronnyi resurs] – Rezhym dostupu: http://westudents.com ua/glavy/16529-126-bezpeka-pdprimstva-v-nformatsyny-sfer-.html

безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування// А.А. Литвинюк – [Електроннийресурс]. – Режим доступу:http://www cvk.gov.ua/visnyk/pdf/2008 4/visnik st 08.pdf

10. Балашов П. А. Оценка рисков информационной безопасности на основе нечеткой логики / П А. Балашов, В П. Безгузиков, Р.И. Кислов // [Електронний ресурс] - Режим доступу: http://www nwaktiv.ru/textstat2/index.htm1

11. Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / Корченко А.Г., Щербина В.П., Казмирчук С.В. // Защита информации – 2012. – №1. – С. 126–139.

12. Батюк А Є Інформаційні системи в менеджменті / А.Є Батюк, З.П. Двуліт, К М. Обельовська, ЇМ Огород ні к, Л.П. Фабрі. – Львів: «ІнтелектЗахід», 2004 – С 343–384.

13. Казакевич О. Ю Предприниматель в опасности: способы защиты Практическое руководство для предпринимателей и бизнесменов / О Ю. Казакевич, Н В Конев. – М. Юрфак МГУ, 2011. – 152 с.

14. Ананский Є. В Защита информации - основа безопасности бизнеса, журнал «Бизнес и безопасность». – 2009. – С 18.

15. Бродська Д. В. Оцінка продуктивності підприємства як складова системи забезпечення його ефективного функціонування / Д В. Бродська [Електронний ресурс] –Режим доступу: http://vestnikdnu сот ua/archive/201264/brodska.html

16. Ортинський В. Л. Економічна безпека підприємств, організацій та установ і В. Л. Ортинський [Електронний ресурс] – Режим доступу: http://westudents.com ua/glavy/16529-126-bezpeka-pdprimstva-v-nformatsyny-sfer-.html