СТАТИСТИКА. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 004.056.5 **JEL Classification: M15, M21**
DOI: https://doi.org/10.32515/2663-1636.2019.3(36).219-228

В.А. Панченко, доц., д-р екон. наук
Центральноукраїнський державний педагогічний університет імені В. Винниченка, м. Кропивницький, Україна

Менеджмент інформаційної безпеки комерційного підприємства

У статті розглянуто передумови формування системи інформаційної безпеки підприємства та визначено особливості управління нею. Розглянуто основні поняття інформаційної безпеки, її призначення та методи вдосконалення інформаційного середовища діяльності підприємства на сучасному етапі розвитку економічної науки. Наведено класифікація і приклади загроз інформаційній безпеці та уніфіковано найбільш уживані методи для забезпечення інформаційної безпеки. Дано опис системи менеджменту інформаційної безпеки. Розглянуто заходи безпеки в контексті ISO 27001. Для забезпечення конфіденційності інформації надано рекомендацій щодо підвищення рівня інформаційної безпеки вітчизняних підприємств.

захист інформації, інформаційна безпека, CISSP, менеджмент інформаційної безпеки, СМІБ, загрози, інформаційні системи

В.А. Панченко, доц., д-р екон. наук
Центральноукраинский государственный педагогический университет имени В. Винниченко, г. Кропивницкий, Украина

Менеджмент информационной безопасности коммерческого предприятия

В статье рассмотрены предпосылки формирования системы информационной безопасности предприятия и определены особенности управления ею. Рассмотрены основные понятия информационной безопасности, ее назначение и методы совершенствования информационной среды деятельности предприятия на современном этапе развития экономической науки. Приведены классификация и примеры угроз информационной безопасности, унифицированы наиболее используемые методы для обеспечения информационной безопасности. Дано описание системы менеджмента информационной безопасности. Рассмотрены меры безопасности в контексте ISO 27001. Для обеспечения конфиденциальности информации предоставлено рекомендации по повышению уровня информационной безопасности отечественных предприятий.

защита информации, информационная безопасность, CISSP, менеджмент информационной безопасности, СМИБ, угрозы, информационные системы

Постановка проблеми. За рахунок масової комп'ютеризації та інформатизації ринку товарів і послуг суб'єкти підприємницької діяльності мають доступ до різноманітної інформації, і тим самим у них полегшуються процеси виробництва, управління і збуту продукції. Однак, останнім часом почастішали випадки електронного шахрайства та кіберзлочинності, що негативно відобразилося на бізнесі.

Гостра проблема інформаційної безпеки комерційних організацій набула важливого значення в сучасних умовах масового застосування комп'ютерних інформаційних систем. Відповідно, надійним засобом захисту підприємства від інформаційних загроз є створення дієвої та ефективної системи захисту.

Аналіз останніх досліджень і публікацій. Нормативно-правові та організаційно-технічні засади інформаційної безпеки відображено працях Б. А. Кормича [4], а також, у ряді міжнародних стандартів, зокрема: ДСТУ ISO/IEC 27001:2015 [3], ISO 27001:2013 [13] тощо.

Теоретичні менеджменту інформаційної безпеки вивчали такі вітчизняні вчені, як: І. А. Маркіна [5], О. В. Матвієнко [6], В. Г. Спрінсян [9], О. І. Турчин [10], а також зарубіжні вчені – А. В. Дорофеев [2], Т. Кемпбелл [12], Г. Ф. Тіптон [14] та інші. Прикладні аспекти управління інформаційною безпекою в організації розгядали у своїх працях такі вчені: С. С. Бучик [1], Е. І. Низенко [7], С. В. Северина [8], О. В. Черевко [11] та інші.

Однак, наукових праці, присвячених менеджменту інформаційної безпеки комерційного підприємства на цей час недостатньо. Певною міро, це пов'язано з тим, що дослідники значну увагу приділяють забезпеченню інформаційної безпеки органів державної влади, але досліджень, присвячених створення дієвого механізму захисту інформаційних систем в комерційних підприємствах, дуже мало, що робить передумови для подальших наукових пошуків. У зв'язку з цим, виникає актуальна потреба у створенні дієвого управлінського механізму захисту інформації та організації інформаційної безпеки на комерційних підприємствах.

Постановка завдання. Метою дослідження є вивчення суті й узагальнення призначення інформаційної безпеки, методів удосконалення інформаційного середовища діяльності підприємства, а також формування системи інформаційної безпеки підприємства та визначення особливостей управління нею.

Виклад основного матеріалу. Управління будь-якою соціально-економічною системою пов'язане з інформаційними процесами. Інформація являє собою зв'язуючу основу процесу управління, оскільки саме вона містить відомості, необхідні для оцінки ситуації та прийняття управлінського рішення [9, с. 9].

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури підприємства, надання різних видів інформаційних сервісів, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів організації, що дозволяють скоротити як фінансові, так і трудові витрати. В інформаційних системах зберігаються і обробляються значні обсяги інформації різного ступеня секретності, тому гостро постає питання про захищеність цих інформаційних систем підприємства від різних загроз безпеці інформації [8, с. 81].

Вчені Е.І. Низенко і В.П. Каленяк вважають, що інформація є важливим стратегічним ресурсом комерційного підприємства. «Згідно з поширеними нині в управлінській літературі поглядами поняття ресурси охоплює не лише людей, капітал, сировину, а й інформацію» [10, с. 5].

Інформація може існувати у різноманітних формах. Вона може бути надрукованою або написаною на папері, зберігатися у електронному вигляді, передаватися поштою або з використанням електронних засобів зв'язку, демонструватися на плівці або бути вираженою усно. Незалежно від форми, засобів розповсюдження і зберігання, інформація є цінним активом будь-якої компанії [2].

Розвиток теорії управління дозволяє розглядати нові самостійні галузі управління, пов'язані з управлінням інформаційними ресурсами, впровадженням і використанням інформаційних технологій в діяльності підприємств і організацій, управлінням процесами опрацювання інформації в організаціях [9, с. 9].

Розвиток комп'ютерних технологій і їх використання в багатьох сферах економіки є на сьогодні одним з головних факторів її ефективності. Проте прогрес в інформаційно-технічній сфері створив і потенційні загрози у вигляді розроблення нових та удосконалення вже відомих методів наукового шпигунства, котрі дозволяють швидко знаходити в комп'ютері необхідні відомості [10, с. 9].

Б.А. Кормич розуміє під інформаційною безпекою «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» [7, с. 15].

Інформаційна безпека підприємства в першу чергу стосується захисту інформаційних систем, особливо функцій які ті виконують (табл. 1).

Таблиця 1 – Функції інформаційних систем

Система маркетингу	Виробничі Системи	Фінансові системи та системи обліку	Система кадрів	Інші системи (напр., ІС керівництва)
Дослідження ринку і прогнозування продаж	Планування обсягів робіт і розробка календарних планів	Управління портфелем замовлень	Аналіз і прогнозування потреби у трудових ресурсах	Контроль за діяльністю організації
Управління продажами	Оперативний контроль і управління виробництвом	Управління кредитною політикою	Ведення архівів записів про персонал	Виявлення оперативних проблем
Рекомендації з виробництва нової продукції	Аналіз роботи обладнання	Розробка фінансового плану	Аналіз і планування підготовки кадрів	Аналіз управлінських і стратегічних ситуацій
Аналіз і встановлення ціни	Участь у формуванні замовлень постачальникам	Фінансовий аналіз і прогнозування	Забезпечення процесу кадрового управління	Вироблення стратегічних рішень
Облік замовлень	Управління ресурсами	Контроль бюджету. Бухгалтерський облік і розрахунок заробітної платні		

Джерело: [9, с. 19].

На основі аналізу наукових джерел [1; 2; 3; 5; 8; 10; 11; 14] перелічимо найбільш поширені види потенційних загроз та небезпек для комерційного підприємства у сфері інформаційної діяльності:

– відсутність копіювання важливих бухгалтерських та організаційно-розпорядчих документів на матеріальних носіях даних;

– відсутність ведення протоколів змін у програмному забезпеченні;

– недобросовісне використання інформації працівниками підприємства;

– відсутність регулювання доступу користувачів до різних типів інформації та баз даних;

– відсутність схем інформаційного забезпечення рівнів управління;

– можливість несанкціонованого втручання в програмне забезпечення та базу даних;

– крадіжка засобів зберігання інформації;

– промислове шпигунство;
– хакерські атаки, шкідливе програмне забезпечення, комп'ютерні віруси;
– піратське програмне забезпечення, не ліцензовані антивірусні програми, відсутність захисного мережевого екрану від Інтернет атак;
– наявність непідзвітних посадових осіб у системі управління підприємством.

Отже, інформаційні системи виконують багато важливих функцій, об'єднувальною є управлінська система.

Виникає необхідність створення інформаційної інфраструктури підприємства на базі парадигми єдиного інформаційного простору підприємства, що передбачає інтеграцію різноманітною науково-технічною, інженерною, фінансовою, маркетинговою і інших видів інформації в рамках єдиної системи. Створення єдиного інформаційного простору дозволяє реалізувати єдиний безперервний цикл інноваційної діяльності підприємства, що гнучко враховує ринкові сигнали в процесі вдосконалення продукції, дозволяє якнайповніше задовольняти потреби клієнтів [13, с. 348].

Під інформаційною безпекою (ІБ) зазвичай розуміють стан (властивість) захищеності ресурсів інформаційної системи в умовах наявності загроз в інформаційній сфері.

Захист інформації – це процес, спрямований на забезпечення інформаційної безпеки. Визначальними факторами інформаційної безпеки є загроза (threat) і ризик (risk). Загрозою називають потенційну причину (подія, порушення, інцидент), що знижує рівень інформаційної безпеки системи, тобто потенційно здатну привести до негативних наслідків (impact) і збитку (loss) системи або організації [5, с. 67].

Інформаційна безпека – механізм захисту, що забезпечує:

1) Конфіденційність: доступ до інформації тільки авторизованих користувачів.
2) Цілісність: достовірність і повноту інформації та методів її обробки.
3) Доступність: доступ до інформації та зв'язаних з нею активів авторизованих користувачів за необхідністю [2].

Для побудови та ефективної експлуатації СЗІБ (система забезпечення інформаційної безпеки) О.В. Черевко рекомендує:

– виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
– врахувати вимоги національного та міжнародного законодавства;
– використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;
– визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;
– рас проділити між підрозділами області відповідальності у здійсненні вимог СЗІБ;
– на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові політики інформаційної безпеки об'єкта захисту;
– реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;
– реалізувати систему менеджменту (управління) інформаційної безпеки (СМІБ);
– використовуючи систему управління організувати регулярний контроль ефективності СЗІБ і при необхідності перегляд і коригування СЗІБ [14].

Дослідниця Северина С.В. робить висновок, що «без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку» [11, с. 160].

Северина С.В. рекомендує для запобігання втрати та витоку таємних даних на підприємстві використовувати такі засоби її захисту: фізичні, апаратні, програмні, апаратно-програмні, законодавчі, криптографічні та організаційні методи [11, с. 159].

Зміст робіт контролю інформаційної безпеки підприємства повинен включати:

– здійснення моніторингу та перевірка процедур та інших засобів контролю ризиків (захисних заходів) для швидкого виявлення помилок в результатах обробки, швидкої ідентифікації порушень безпеки, надання керівництву інформації, сприяння виявленню подій небезпеки і запобігання виникнення інцидентів загроз інформаційній та іншим видам безпеки підприємства за допомогою використання відповідної системи критеріїв;

– регулярні перевірки ефективності системи менеджменту інформаційної безпеки (включаючи дотримання політики і досягнення цілей системи менеджменту інформаційної безпеки, перевірку засобів контролю безпеки), враховуючи результати аудитів безпеки, інцидентів, результати вимірювань ефективності, пропозиції усіх зацікавлених сторін;

– перегляд оцінки рівня ризику через заплановані інтервали часу, а також визначення залишкових ризиків та ідентифікація прийнятних рівнів ризику відповідно до змін в організації та в її операційному і бізнес-середовищі;

– здійснення внутрішніх аудитів діяльності системи менеджменту інформаційної безпеки;

– здійснення перевірки керівництвом системи менеджменту інформаційної безпеки для підтвердження адекватності сфери її дії і ефективності заходів щодо вдосконалення системи менеджменту інформаційної безпеки [8, с. 86].

В таблиці 2 наведено характеристику основних міжнародних стандартів з управління інформаційними ризиками на комерційному підприємстві.

Таблиця 2 – Міжнародні стандарти з керування методів для визначення інформаційних ризиків та їх коротка характеристика

Стандарт	Назва стандарту	Коротка характеристика
1	2	3
ISO/IEC 27002-2012	Інструкція з менеджменту інформаційної безпеки для телекомунікаційних організацій	Цей стандарт надає додаткові рекомендації з реалізації та менеджменту ІБ в телекомунікаційних організаціях. Визначає цілі, вимоги оцінки ризику до системи ІБ та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, поліпшення менеджменту ІБ
ISO/IEC 27003-2012	Інструкція з реалізації системи менеджменту ІБ	У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІБ відповідно зі стандартом ISO/IEC 27001:2005, який розглядає процес визначення та розробку СМІБ від початку до стану впровадження

Продовження таблиці 2

1	2	3
ISO/IEC 27004-2011	Менеджмент інформаційної безпеки вимірювання	Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІБ. Процес вимірювання реалізується у вигляді програми, пов'язаний з ІБ. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІБ, а також визначення пріоритетів дій, спрямованих на удосконалення або зміну цих процесів
ISO/IEC 27005-2010	Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику	Цей стандарт поданий у вигляді додатку прикладу типових загроз, уразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків насамперед асоціюється з британським стандартом BS 7799, а саме з його двома частинами: першою – BS 7799-1 «Звіт правил з менеджменту безпеки інформації» та другою – BS 7799-2 «Системи менеджменту безпекою інформації», у яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов'язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту BS 7799-3 «Настанови з менеджменту ризиками безпеки інформації»
ISO/IEC TR 13335-2: 1997	Настанови з керування безпекою інформаційних технологій (IT)	Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (IT). Кваліфікація осіб, відповідальних за безпеку IT у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій

Джерело: [4, с. 222].

ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги). Цей стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На проектування та впровадження

системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги щодо безпеки, застосовувані організаційні процеси, розмір і структура організації.

Система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності й доступності інформації за допомогою запровадження процесу управління ризиками та надає впевненості зацікавленим сторонам, що ризиками належним чином управляють [6, с. 5].

Розглянемо сутність та мету сфери інформаційного менеджменту.

Сфера інформаційного менеджменту – це сукупність необхідних для управління рішень на всіх етапах життєвого циклу підприємства, що включає дії та операції, пов'язані з інформацією у різних формах і станах, та з підприємством у цілому. При цьому, вирішуються завдання визначення цінності й ефективності використання інформації і знань (щоб усі менеджери отримували тільки релевантну інформацію), а також цінності та інших ресурсів підприємства, що входять у контакт із інформацією: технологічних, кадрових, фінансових [12, с. 15].

Завдання інформаційного менеджменту:

– формування інформаційної сфери підприємства (організації);
– розвиток інформаційної системи та забезпечення її обслуговування;
– планування в інформаційному середовищі;
– формування організаційної структури у світлі інформатизації;
– використання інформаційних систем;
– формування інноваційної політики та реалізація інноваційних програм;
– управління персоналом в інформаційній системі підприємства;
– управління капіталовкладеннями в інформаційну систему підприємства;
– формування і забезпечення комплексного захисту інформаційних ресурсів [12, с. 15-16].

Метою інформаційного менеджменту є забезпечення ефективного розвитку комерційного підприємства за допомогою оперативного і гнучкого регулювання різних видів інформаційної діяльності (пошук, збір, аналіз, синтез, обробка, передача, зберігання та використання різної інформації).

У сфері інформаційних технологій менеджер з безпеки інформаційної діяльності комерційного підприємства повинен бути добре обізнаним з таких основних питань:

– комп’ютерне обладнання, конфігурація телекомунікаційних систем та мереж;
– введення, виведення та пошук інформації;
– оцінка ефективності комп’ютерних систем;
– тенденції розвитку інформаційних технологій;
– методи та способи захисту інформації та комп’ютерних мереж;
– проектування баз даних та управління ними;
– аналіз, налаштування і контроль за інформаційними системами;
– технології обробки та передачі інформації;
– основи управління системами телекомунікацій.

Аналіз напрацювань в даній сфері дозволив визначити, що стандартній системі управління інформаційною безпекою підприємства притаманні всі загальні для систем менеджменту елементи. При цьому, досвід використання стандартизованих вимог до системи менеджменту інформаційної безпеки визначив основні фактори для забезпечення інформаційної безпеки на сучасному підприємстві:

– політика інформаційної безпеки, цілі та заходи, що відображають цілі бізнесу суб'єкта господарювання;

– підхід і структура реалізації, підтримки моніторингу та вдосконалення інформаційної безпеки, узгоджуються з культурою організації;

– підтримка і прихильність керівництва всіх рівнів;

– розуміння вимог інформаційної безпеки, оцінка ризику та наявність ризик-менеджменту;

– ефективні заходи щодо формування компетентності з питань інформаційної безпеки для належного усвідомлення;

– поширення настанов (інструкцій) з політики та стандартів інформаційної безпеки серед всіх керівників, службовців та інших контрагентів;

– забезпечення фінансування заходів менеджменту інформаційної безпеки;

– забезпечення відповідної інформованості, навчання і освіти;

– встановлення ефективного процесу менеджменту інцидентів інформаційної безпеки;

– оцінювання системи, яке використовується для оцінки ефективності функціонування менеджменту інформаційної безпеки і пропозицій щодо вдосконалення [8, с. 85].

Отже, система управління інформаційною безпекою комерційного підприємства, побудована на основі вимог міжнародних стандартів ISO, дозволить менеджерам організувати ефективну систему для створення, управління, контролю і захисту важливої інформації та документів.

Висновки та перспективи подальших досліджень. За результатами проведеного дослідження, присвяченого проблемі менеджменту інформаційної безпеки комерційного підприємства, було наведено визначення поняттю «Менеджмент інформаційної безпеки», виділено функції інформаційних систем підприємства, а також проаналізована основні міжнародні стандарти з управління інформаційною безпекою організації.

Виявлено переваги для комерційного підприємства від впровадження системи управління інформаційної безпеки:

– захист інформації та документів від крадіжок;

– підвищення довіри з боку ділових партнерів, впевнених в захисті їхньої комерційної інформації, секретів виробництва та бізнесу;

– покращення позитивного іміджу підприємства;

– посилення конкурентних переваг за рахунок захисту інформації;

– створення дієвого управлінського механізму для виявлення ризиків та управління ними при забезпеченні інформаційної безпеки комерційного підприємства.

Таким чином встановлено, що між системою інформації і структурою управління в комерційному підприємстві існує органічний взаємозв'язок і взаємозалежність.

Перспективою подальших досліджень може бути побудова моделі системи управління інформаційною безпекою на комерційному підприємстві.

Список літератури

1. Бучик С. С., Шалаєв В. О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. *Наукоємні технології*. 2017. № 3. С. 215-225. URL: http://nbuv.gov.ua/UJRN/Nt_2017_3_6. (дата звернення 19.11.2019)
2. Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции *Вопросы кибербезопасности*. 2014. №1 (2). С. 67-73.

3. ДСТУ ISO/IEC 27001:2015 Методи захисту системи управління інформаційною безпекою: вимоги. [Чинний від 18-12-2015]. Київ, 2015. 28 с. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення 20.10.2019) (Національний стандарт України)
4. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здоб. наук. ступеня д. юр. наук : спец. 12.00.07 / ХНУВС. Харків, 2004. 42 с.
5. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. №3 (1). С. 80-88 . URL: http://nbuv.gov.ua/UJRN/piprp_2016_3(1)_18. (дата звернення 24.11.2019)
6. Матвієнко О. В., Цивін М. Н. Основи менеджменту інформаційних систем : навчальний посібник. Київ : Центр навчальної літератури, 2005. 176 с.
7. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва : навч. посіб. Київ : МАУП, 2006. 134 с.
8. Северина С. В. Інформаційна безпека та методи захисту інформації *Вісник Запорізького національного університету. Економічні науки.* 2016. №1. С. 155-161. URL: http://nbuv.gov.ua/UJRN/Vznu_eco_2016_1_21. (дата звернення 28.11.2019)
9. Спрінсян В. Г., Бірюкова Т. Л. Ресурси та технології інформаційного менеджменту : навчальний посібник. Одеса : ОНПУ, 2012. 248 с.
10. Турчин О. І. Інформаційна безпека процесів менеджменту інтегрованих систем. *Моделювання регіональної економіки*. 2010. №2. С. 347-352. URL: http://nbuv.gov.ua/UJRN/Modre_2010_2_42. (дата звернення 25.10.2019)
11. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. *Ефективна економіка*. 2014. №5. URL: http://nbuv.gov.ua/UJRN/efek_2014_5_103. (дата звернення 12.11.2019)
12. Campbell T. Practical Information Security Management : A Complete Guide to Planning and Implementation. New York-Australia : «Science+Business». 2015. 385 p.
13. ISO 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. URL: http://www.teamprevent.com.ua/ua/poslugi/sistemi_menedzhmentu/iso_27001_sistema_menedzhmentu_ informaciinoji_bezpeki.html (18.11.2019)
14. Tipton Harold F., Micki Krause Information security management handbook. 6th ed. USA : Boca Raton : «Taylor & Francis Group». 2017. 458 p.

References

1. Buchyk, S. S. & Shalaiev, V. O. (2017). Analiz instrumental'nykh metodiv vyznachennia ryzykiv informatsijnoi bezpeky informatsijno-telekomunikatsijnykh system [Analysis of instrumental methods for determining information security risks of information and telecommunication systems.]. *Naukoiemni tekhnolohii – Technology-intensive. 3*, 215-225 Retrieved from http://nbuv.gov.ua/UJRN/Nt_2017_3_6. (data zvernennja 19.11.2019) [in Ukrainian].
2. Dorofeev, A. V. & Markov, A. S.(2014). Menedzhment informacionnoj bezopasnosti: osnovnye koncepcii [Information security management: basic concepts]. *Voprosy kiberbezopasnosti – Cybersecurity issues, 1 (2),* 67-73 [in Russian].
3. Metody zakhystu systemy upravlinnia informatsijnoiu bezpekoiu: vymohy [Methods of protection of information security management system: requirements] (2015). *DSTU ISO/IEC 27001:2015 from18th December 2015*. Kyiv: Natsional'nyj standart Ukrainy. Retrieved from https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015 [in Ukrainian].
4. Kormych, B. A. (2004). Orhanizatsijno-pravovi osnovy polityky informatsijnoi bezpeky Ukrainy [Organizational and legal bases of information security policy of Ukraine]. *Extended abstract of Doctor's thesis*. KhNUVS. Kharkiv, 2004. 42 c. . [in Ukrainian].
5. Markina, I. A. & Diachkov, D. V. (2016). Osnovy formuvannia systemy menedzhmentu informatsijnoi bezpeky pidpryiemstva [Fundamentals of formation of enterprise information security management system]. *Problemy i perspektyvy rozvytku pidpryiemnytstva – Problems and prospects of entrepreneurship development, 3 (1),* 80-88. Retrieved from http://nbuv.gov.ua/UJRN/piprp_2016_3(1)_18. (data zvernennja 24.11.2019) [in Ukrainian].
6. Matviienko, O. V. & Tsyvin, M. N. (2005). *Osnovy menedzhmentu informatsijnykh system* [*Fundamentals of Information Systems Management*]. Kyiv : Tsentr navchal'noi literatury [in Ukrainian].
7. Nyzenko, E. I. & Kaleniak, V. P. (2006). *Zabezpechennia informatsijnoi bezpeky pidpryiemnytstva [Ensuring information security of entrepreneurship]*. Kyiv : MAUP [in Ukrainian].
8. Severyna, S. V. (2016). Informatsijna bezpeka ta metody zakhystu informatsii [Information security and methods of information protection]. *Visnyk Zaporiz'koho natsional'noho universytetu. Ekonomichni nauky*

– *Visnyk of Zaporizhzhya National University. Economic sciences*, *1*, 155-161. Retrieved from http://nbuv.gov.ua/UJRN/Vznu_eco_2016_1_21 [in Ukrainian].
9. Sprinsian, V. H. & Biriukova, T. L. (2012). Resursy ta tekhnolohii informatsijnoho menedzhmentu *[Information management resources and technologies: a textbook]*. Odesa : ONPU [in Ukrainian].
10. Turchyn, O. I. (2010). Informatsijna bezpeka protsesiv menedzhmentu intehrovanykh system [Information security of integrated systems management processes]. *Modeliuvannia rehional'noi ekonomiky – Modeling of regional economy*, *2*, 347-352. Retrieved from http://nbuv.gov.ua/UJRN/Modre_2010_2_42 [in Ukrainian].
11. Cherevko, O. V. (2014). Teoretychni zasady poniattia informatsijnoi bezpeky ta klasyfikatsiia zahroz systemi informatsijnoho zakhystu [Theoretical principles of the concept of information security and classification of threats to the information security system]. *Efektyvna ekonomika – An efficient economy*, *5*. Retrieved from http://nbuv.gov.ua/UJRN/efek_2014_5_103 [in Ukrainian].
12. Campbell, T. (2015). Practical Information Security Management : A Complete Guide to Planning and Implementation. New York-Australia : «Science+Business» [in English].
13. Information technology – Security techniques – Information security management systems – Requirements. (2019). *ISO 27001:2013 from 18th November 2019*. Retrieved from http://www.teamprevent.com.ua/ua/poslugi/ sistemi_menedzhmentu/iso_27001_sistema_menedzhmentu_informaciinoji_bezpeki.html [in Ukrainian]
14. Tipton Harold F., Micki Krause (2017). Information security management handbook. 6th ed. USA : Boca Raton : «Taylor & Francis Group» [in English].

Volodymyr Panchenko, Associate Professor, Doctor in Economics (Doctor of Economic Sciences)
Central Ukrainian Pedagogical University named after Volodymyr Vynnychenko, Kropyvnytskyi, Ukraine

Information Security Management of a Commercial Enterprise

The basic concepts of information security such as properties, threats, vulnerabilities, risks, controls are reviewed. The classification and examples of information security threats are given. The information security management system is described. The measures of security in the context of ISO 27001 are discussed.

The article considers the preconditions of enterprise information security and the control features are defined by it, that associated with the continuous development of enterprise information infrastructure, the provision of various types of information services, automation of financial and operational performance, as well as the business processes of modern organizations.

It was determined that the purpose of information management is to ensure the effective development of a business enterprise through the prompt and flexible regulation of various types of information activities (search, collection, analysis, synthesis, processing, transmission, storage and use of various information).

The advantages for the commercial enterprise from the introduction of the information security management system are revealed: (a) protecting information and documents against theft; (b) increasing the confidence of business partners who are confident in protecting their business information, production secrets and business; (c) improving the positive image of the company; (d) increasing competitive advantage by protecting information; (e) creating an effective management mechanism for identifying and managing risks while ensuring information security of a business enterprise.

Determined concept, purpose and methods of information security improvements of enterprise information environment at the present stage of development economics. Classification and unification of the most commonly used methods for information security. In order to ensure the confidentiality of information were provided recommendations for improving the information security of domestic enterprises.

threat, information systems, information security, security controls, CISSP, information security management, ISMS, threats, information systems

Одержано (Received) 11.12.2019 *Прорецензовано (Reviewed) 18.12.2019*
Прийнято до друку (Approved) 23.12.2019