РОЗДІЛ 10. ЕКОНОМІЧНА БЕЗПЕКА

ФОРМУВАННЯ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
FORMATION OF INFORMATIONAL SECURITY MODEL

УДК 681.3.06

Дячков Д.В.
к.е.н., доцент кафедри менеджменту
Полтавська державна аграрна академія

В статті обумовлена актуальність формування моделі інформаційної безпеки, що пов'язано з розвитком глобального інформаційного суспільства та якісною зміною способів зберігання та обробки інформаційних ресурсів. На основі узагальнення було запропоновано структурну модель інформаційної безпеки систем, що базується на положеннях комплексного підходу. Пропонована структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах полягає в аналізі її основних компонентів: визначенні головних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та цілей захисту. Запропоновано формалізовану модель інформаційної безпеки, яка є функцією з множини області значень складових системи інформаційної безпеки і передбачає, що постійне зростання потреби в інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

Ключові слова: *захист інформаційних ресурсів, формалізована модель інформаційної безпеки, комплексний підхід, стан системи, структурна модель, джерела інформації, вразливості, суб'єкти безпеки.*

В статье обусловлена актуальность формирования модели информационной безопасности, которая связана с развитием глобального информационного общества и качественным изменением способов хранения и обработки информационных ресурсов. На основе обобщения было предложено структурную модель информационной безопасности систем, основанную на положениях комплексного подхода. Предлагаемая структурная модель предполагает, что решение проблемы безопасности в информационных системах заключается в анализе ее основных компонентов: определении главных задач защиты информации, определении субъектов информационных процессов, классификации основных возможных угроз безопасности, определении уровней уязвимости информационных систем, определении источников информации, ознакомлении с особенностями источников угроз, исследовании способов и направлений защиты и целей защиты. Предложено формализованную модель информационной безопасности, которая является функцией из множества областей значений составляющих систему информационной безопасности, предполагает, что постоянный рост потребности в информации обусловливает необходимость наращивания и эффективного использования информационных ресурсов, формирования информационного потенциала организационных образований, выступает основной предпосылкой изменения состояния системы информационной безопасности, перестройки или совершенствовании ее модели.

Ключевые слова: *защита информационных ресурсов, формализованная модель информационной безопасности, комплексный подход, состояние системы, структурная модель, источники информации, уязвимости, субъекты безопасности.*

The article substantiates the topical problem of forming informational security model, caused by development of global informational society and qualitative changes in ways of informational resources storing and processing. The offered structural model envisages decision of the security problem in informational systems is in analysis of its main components: definition of basic tasks of protection of information, definition of subjects of informational processes, classification of basic possible security threats, definition of levels of vulnerability of informational systems, definition of sources of information, familiarization with peculiarities of sources of threats, research of ways and directions of protection and goals of protection. Based on the integration of these approaches it was suggested formalized model of informational security, which is a function of the data components multitude of informational security system. It also determines that steady growth of needs in information causes necessity of accumulating and using informational resources. It leads to form information potential of organization, that enables to change the conditions of informational security systems as well as improve its model.

Key words: *protection of information resources, formalized model of information security, complex approach, state of the system, structural model, sources of information, vulnerabilities, security subjects.*

Постановка проблеми. Процес формування глобального інформаційного суспільства призвів до якісної зміни способів зберігання і обробки інформаційних ресурсів. Саме інтелектуальні інформаційні технології дозволяють суб'єктам, що не володіють достатніми матеріальними ресурсами, поставляти на світовий ринок інформаційні послуги, продукти, технології. З іншого боку, розвиток комп'ютерних мереж та інформаційних технологій викликав різке збільшення порушень авторських прав власників інформації. Створення системи управління захистом інформації ґрунтується на послідовному визначенні об'єктів управління, цілей і задач управління, показників і крите-

ріїв ефективності управління, функцій управління, складу системи та організаційної структури управління, на розробці методів і засобів управління. У зв'язку з цим, проблема забезпечення інформаційної безпеки і захист інформаційних систем від несанкціонованого доступу набула особливої актуальності.

Аналіз останніх досліджень та публікацій. Етимологічній проблематиці поняття «інформаційної безпеки», в окремих предметних областях дослідження, присвячені праці відомих вчених, зокрема: Гузалюка М. [1], Данільяна О. [2], Калюжного Р. [1], Ковтуна С. [3], Тер-Акопова А. [4] та інших.

Про принципову можливість застосування систем інформаційної безпеки поряд з іншими методами захисту соціально-економічних процесів згадували у свої працях Шамраєв А. [5], Морозов А.[6], Родічєв Ю.[7].

Вагомий внесок в розвиток підходів до формування моделі інформаційної безпеки несли вітчизняні вчені та відомі зарубіжні теоретики: Зегжда Д. [8], Харісон М. [9], Потій А. [10], Родічєв А. [7], Родієчев Ю. [7] та ін.

Формулювання цілей статті. Поняття інформаційної безпеки в сучасній термінології досі не є визначеним через відсутність єдиної методологічної основи, на базі якої можуть бути визначені її сутність, ступінь необхідності використання та межі застосування [5]. З методологічної точки зору, при аналізі проблем інформаційної безпеки необхідно виявити суб'єкти інформаційних відносин та їх інтереси, пов'язані з використанням інформаційних систем, визначити завдання захисту інформації, основні загрози безпеці і можливі засоби захисту від них. Вищезазначене потребує розробки багатовимірної моделі інформаційної безпеки [10, с. 129]. Проте, більшість підходів до формування моделі інформаційної безпеки є односторонніми: характеризуючи структуру моделі, не відображають процес захисту інформації та інформаційних ресурсів; описуючи послідовність процесу формування моделі, не враховують особливості побудови бізнес-процесів; при спробі формалізації моделі інформаційної безпеки – не враховують її адитивні властивості, тощо.

Метою дослідження є формування моделі інформаційної безпеки основаної на комплексному підході, що забезпечить практичність її побудови та застосування.

Виклад основного матеріалу. Створення моделі управління захистом інформації ґрунтується на послідовному визначенні об'єктів управління, цілей і завдань управління, показників і критеріїв ефективності управління, функцій управління, складу системи та організаційної структури управління, на розробці методів і засобів управління.

Проблеми інформаційної безпеки істотно залежать від типу інформаційних систем і сфери їх застосування. У локальних системах малого масштабу систему захисту побудувати набагато простіше, ніж в системах розподіленого типу, що пояснюється особливостями цих систем, основними з яких є: територіальна розосередженість компонентів системи і як наслідок наявність обміну інформацією між ними; широкий спектр способів подання, зберігання і передачі інформації; одночасна участь в процесах опрацювання інформації великою кількістю користувачів з різними правами доступу; використання різнорідних програмно-технічних засобів обробки і систем телекомунікацій [10]. Саме тому запропонована структурна модель інформаційної безпеки систем розподіленого типу, яка відображена на рис. 1.

Структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі наступних основних компонентів: визначення основних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та звичайно цілей захисту. Забезпечення безпеки інформації полягає у вирішенні трьох взаємопов'язаних завдань: конфіденційність, цілісність і доступність.

Завдання забезпечення конфіденційності полягає в захисті інформації в процесі її створення, зберігання, обробки та обміну від ознайомлення з нею особами, які не мають права доступу до неї. Завдання щодо забезпечення цілісності полягає в захисті від навмисної або ненавмисної зміни інформації та алгоритмів її обробки особами, які не мають на те права. Забезпечення доступності полягає в наданні користувачам всієї наявної в системі інформації відповідно до встановлених їм правам [7, с. 17].

Основними суб'єктами в інформаційних процесах є: автори і власники інформації, авторизовані користувачі інформації, неавторизовані особи (особи, які намагаються отримати самовільний доступ до інформації), окремі співробітники або колективи, які беруть участь в розробці, забезпеченні працездатності програмно-технічних засобів інформаційних систем і наповненні системи інформацією. Системи захисту повинні забезпечувати захист прав авторів і власників інформації та одночасно надавати доступ до інформації користувачам відповідно до їх прав.

Під загрозою безпеки інформаційних систем розуміється потенційно можлива дія, подія або процес, який за допомогою впливу на інформацію та інші компоненти системи може завдати шкоди інтересам суб'єктів.

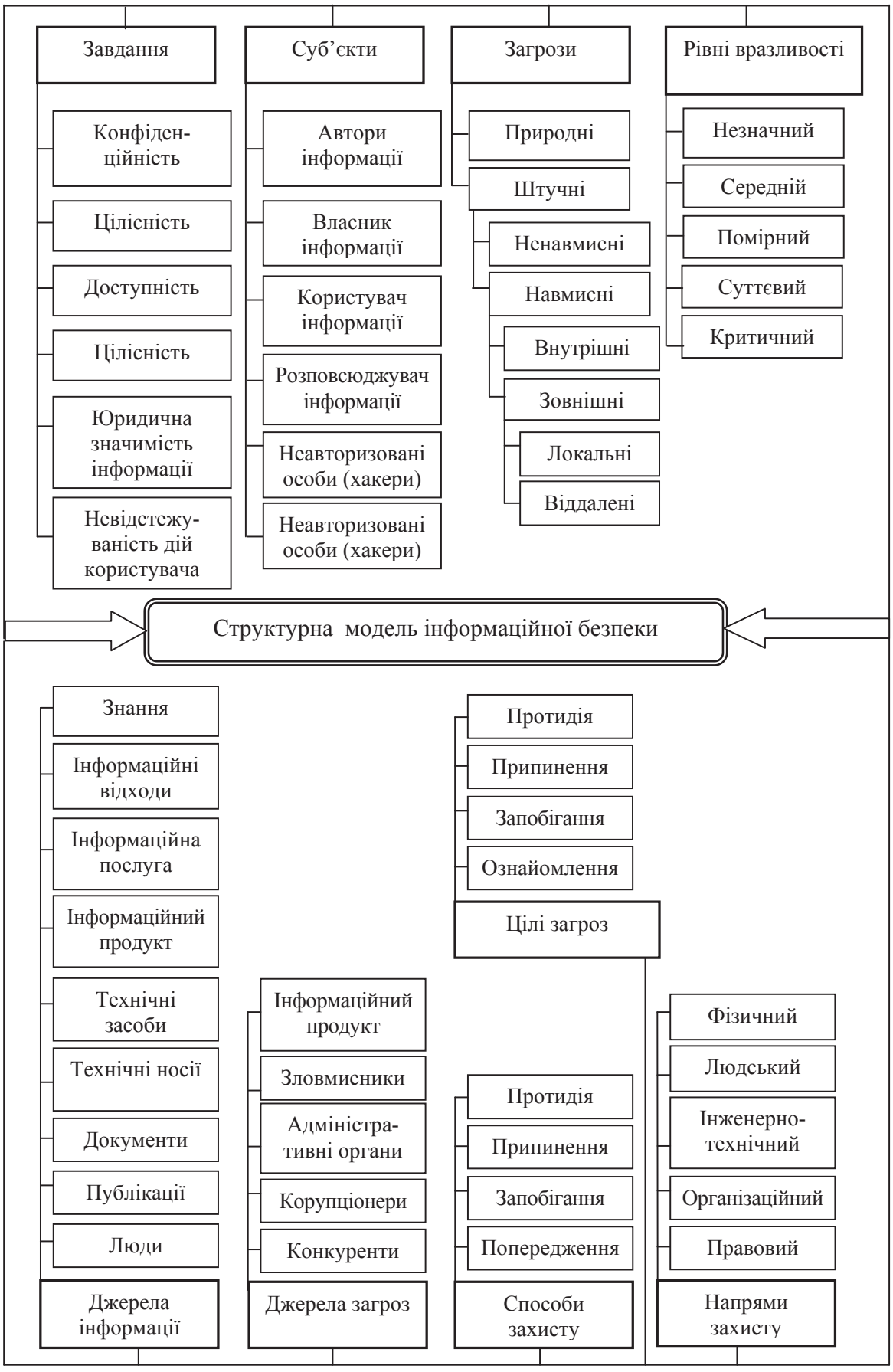

Рис. 1. Структурна модель інформаційної безпеки

Джерело: узагальнена та доповнена на основі [4, 6, 7, 10]

Джерелами загроз виступають конкуренти, злочинці, корупціонери, адміністративно-управлінські органи.

Джерела загроз переслідують при цьому наступні цілі: ознайомлення з відомостями, що охороняються, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Неправомірне заволодіння конфіденційною інформацією можливо шляхом її розголошення джерелами відомостей, за рахунок витоку інформації через технічні засоби та через несанкціонований доступ до відомостей, що охороняються.

Джерелами конфіденційної інформації є люди, їх знання, документи, публікації, технічні носії інформації, технічні засоби забезпечення виробничої та трудової діяльності, продукція, послуги і відходи виробництва.

Основними напрямками захисту інформації є правовий, організаційний, інженерно-технічний, людський, фізичний захист інформації як індикатори комплексного підходу до забезпечення інформаційної безпеки.

Засобами захисту інформації є фізичні засоби, апаратні засоби, програмні засоби та криптографічні методи. Останні можуть бути реалізовані як апаратно, програмно, так і змішано-програмно-апаратними засобами.

В якості засобів захисту виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидія несанкціонованому доступу.

Окрім системного підходу, доцільно врахувати і положення процесного підходу до моделювання систем інформаційної безпеки. Сутність процесного підходу до формування моделі інформаційної безпеки полягає в тому, що захист інформації розглядається як особливий вид діяльності в організації, який здійснюється при моделюванні, проектуванні як сукупність процесів захисту інформації:

- наявність мети процесу, тобто бажаного результату захисту інформації, що досягається при здійсненні процесу;
- зміни предметної області, в якій реалізується процес. По суті, реалізація процесу завжди пов'язана зі зміни системи та є цілеспрямованим переходом цієї системи з існуючого в бажаний стан;
- обмеженість необхідних ресурсів на виконання операцій і дій, що складають процес;
- безперервність процесу. Процес є модель функції захисту, яка здійснюється організацією протягом усього свого існування;
- комплексність та розмежування процесу. Комплексність процесу передбачає врахування всіх внутрішніх і зовнішніх факторів, які прямо або опосередковано впливають на розвиток процесу і результати процесу [10, с. 128-129].

У той же час кожен процес має чітко визначені межі предметної області, наприклад процес аналізу загроз, процес сертифікації засобів захисту, процеси стратегічного управління безпекою тощо.

Формалізуючи модель інформаційної безпеки у математичному вигляді, доцільно визначити її функціональну залежність від завдань захисту інформації, суб'єктів інформаційних процесів, загроз безпеки, рівнів вразливості інформаційних систем, джерел інформації, джерел загроз, способів захисту, напрямів захисту, цілей захисту:

$$S_{mis} = f\,[\{W(MIS_{sub})\}, \{W(MIS_{task})\}, \{W(MIS_{threats})\}, \{W(MIS_{level})\}, \{W(MIS_{sourceinf})\}, \{W(MIS_{sourcethreat})\}, \{W(MIS_{wayprotect})\}, \{W(MIS_{directprotect})\}\ \{W(MIS_{goal})\}], \quad (1)$$

де S_{mis} – стан системи інформаційної безпеки;

$\{W(MIS_{sub})\}$ – сукупність суб'єктів системи інформаційної безпеки;

$\{W(MIS_{task})\}$ – сукупність завдань системи інформаційної безпеки;

$\{W(MIS_{threats})\}$ – сукупність загроз системи інформаційної безпеки;

$\{W(MIS_{level})\}$ – рівні вразливості системи інформаційної безпеки;

$\{W(MIS_{sourceinf})\}$ – сукупність джерел інформації системи інформаційної безпеки;

$\{W(MIS_{sourcethreat})\}$ – сукупність джерел загроз системи інформаційної безпеки;

$\{W(MIS_{wayprotect})\}$ – сукупність способів захисту інформаційних ресурсів;

$\{W(MIS_{directprotect})\}$ – сукупність напрямів захисту інформаційних ресурсів;

$\{W(MIS_{goal})\}$ – сукупність цілей захисту інформаційних ресурсів.

Інформаційна безпека є функцією з множини області значень складових системи інформаційної безпеки. Постійне зростання потреби в інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

При будь-якій зміні стану організації як соціально-економічної системи, зміну моделі системи інформаційної безпеки (ΔS_{mis}) можна виразити рівнянням:

$$\Delta S_{mis} = \Delta S_{in}\ ;\ \Delta S_{ext}, \quad (2)$$

де ΔS_{in} – зміна стану системи інформаційної безпеки через взаємодію із зовнішнім середовищем;

ΔS_{ext} – зміна стану системи.

Вищезазначена формалізація моделі процесу інформаційної безпеки розглядати захист інформації як сукупність процесів. Захист інформації здійснюється відповідно до заздалегідь визна-

ченої та постійно змінюваної мети захисту, яка пов'язана з затратами фінансових, енергетичних, трудових, матеріальних та інших ресурсів, з врахуванням обмежень зовнішнього середовища. Бажаний результат захисту інформації досягається більш ефективно, в тому випадку, якщо пов'язані ресурси і діяльність розглядаються і управляються як процес. Процес, як категорія, використовується як засіб структурування діяльності суб'єкту захисту інформації.

Висновки. Побудована модель захисту інформації для інформаційних систем розподіленого типу, дозволяє визначити основні завдання щодо забезпечення безпеки, виявити суб'єкти в інформаційних процесах, визначити типи загроз і рівнів уразливості. В кінцевому рахунку вона дозволяє побудувати ефективну систему захисту інформації, застосувати адекватні засоби і методи безпеки на всіх рівнях інформаційних процесів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Калюжний Р. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міністерсово освіти і науки України, СБУ. – К. – 2000. – С. 17-21.

2. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. – Х.: «ФОЛІО», 2002. – 296 с.

3. Ковтун С. В. Інформаційна безпека: підручник / С.В. Ковтун. – Харків. Вид. ХНЕУ, 2009. – 368 с.

4. Тер-Акопов А. А. Безопасность человека / Тер-Акопов А. А. – М.: Изд-во МНЭПУ. – 1998. – 256 с.

5. Шамраев А. В. Правовое регулирование информационных технологий (анализ проблем и основные документы) / А. В. Шамраев. – Версия 1.0. М.: Статут, Интертех, БДЦ-пресс, 2003. – 1013 с.

6. Морозов А. В. Сохранность ресурсов автоматизированных информационных финансово-экономических и бухгалтерских систем / А. В. Морозов, Ю. А. Родичев // Междунар. науч.-техн. конф. «Измерение, контроль, информатизация». – ИКИ-2000. – Барнаул, 2000. – С . 148-151.

7. Родичев А. Ю. Системная модель защиты информации информационных систем распределенного типа / А. Ю. Родичев, Ю. А. Родичев // Вестник СамГУ. Естественнонаучная серия. – 2003. – Второй спец. выпуск. – С. 15-20.

8. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.

9. Harrison M. Protection in operating systems / M. Harrison, W. Ruzzo, J. Ullman // Communication of ACM. – 1976. – № 19(8). – P. 461-471.

10. Потий А. В. Формальная модель процесса защиты информации / А. В. Потий // Радіоелектрон. і комп'ют. системи. – 2006. – №5. – С. 128-133.