УДК 021.21

О. В. БОБРИШЕВА

СТРУКТУРНО-ФУНКЦІОНАЛЬНА МОДЕЛЬ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БІБЛІОТЕКИ

Визначено структурно-функціональні взаємозв'язки між основними елементами системи інформаційної безпеки бібліотеки. На основі детального аналізу базових підсистем запропоновано концептуальну модель структурно-функціонального типу.

Ключові слова: *інформаційне суспільство, безпека інформаційного середовища, інформаційна безпека бібліотек, концептуальна модель інформаційної безпеки.*

Определены структурно-функциональные взаимосвязи между основными элементами системы информационной безопасности библиотеки. На основе детального анализа базовых подсистем предложена концептуальная модель структурно-функционального типа.

Ключевые слова: *информационное общество, безопасность информационной среды, информационная безопасность библиотек, концептуальная модель информационной безопасности.*

The article defines structural and functional interconnections between basic elements of the system of information security of the library. The conceptual model of structural and functional type designed on the base of detailed analysis of basic subsystems has been proposed.

Key words: *information society, security of information environment, information security of libraries, conceptual model of information security.*

Формування системи інформаційної безпеки — одна з необхідних умов успішного та перспективного функціонування бібліотек, які дедалі більше використовують глобальні інформаційні ресурси, автоматизовані технології, зберігають електронні дані. Нові стратегії діяльності бібліотечних закладів, які базуються на концепції надання вільного доступу до інформації, загальносвітові тенденції розвитку теоретико-методологічних і практичних засад проблеми розвитку інформаційного середовища, зумовлюють функціонування системи інформаційної безпеки бібліотеки (СІББ) як елементу метасистеми «інформаційна безпека суспільства і держави». Формуючи власну систему інформаційної безпеки, бібліотека є одним із суб'єктів забезпечення інформаційної безпеки суспільства, яка, у свою чергу, є інфраструктурною складовою національної безпеки України [2].

Різноманітність зовнішніх і внутрішніх факторів діяльності бібліотечно-інформаційних закладів зумовлює специфіку їхньої системи інформаційної безпеки. Тому розробка теоретико-методологічних засад цієї предметної галузі повинна мати

узагальнюючий характер і відповідати різним чинникам бібліотечно-інформаційної діяльності. Отже, для вивчення складного та багатоаспектного процесу забезпечення інформаційної безпеки публічної бібліотеки доцільно застосувати метод моделювання як один із загальнонаукових методів дослідження соціально-комунікаційних феноменів.

Питання в галузі моделювання системи інформаційної безпеки викладені в працях таких вітчизняних і зарубіжних учених: В. Асанович, Г. Маньшин, Г. Ньюбі, Ю. Плотинський, В. Ярочкін та ін. Незважаючи на численні публікації з питань розробки концептуальної моделі системи інформаційної безпеки, що стосуються здебільшого впровадження комплексу стандартів ISO/IEC серії 27000, питання методології моделювання системи інформаційної безпеки бібліотек у наукових дослідженнях висвітлені недостатньо.

Мета статті — визначення структурно-функціональних взаємозв'язків між базовими елементами інформаційної безпеки бібліотеки та розробка на їх основі концептуальної моделі.

Елементи системи «інформаційна безпека бібліотеки» можна виокремити завдяки термінологічному аналізу поняття «інформаційна безпека» та врахуванню функцій і завдань бібліотечно-інформаційної інституції. Це, передусім, безпека електронних ресурсів бібліотечно-інформаційних систем, що забезпечується за допомогою захисту інформації від несанкціонованого доступу, пошкодження, модифікації та втрати. Невід'ємною складовою СІББ є захист авторських прав і правовий захист інтелектуальної власності безпосередньо. Важлива також інформаційна безпека користувачів та персоналу. СІББ повинна передбачати захист особистості від негативної інформації, гарантувати її точність і надійність, забезпечувати захист особистих даних користувачів та персоналу. Взаємозв'язок і взаємовплив між запропонованими базовими підсистемами визначаються методами та засобами реалізації складових системи СІББ.

Отже, інформаційна безпека бібліотеки являє собою складну систему, тому для її детального вивчення необхідно розробити структурно-функціональну концептуальну модель, завдяки якій об'єкт розглядається як цілісна система, що поділяється на складові, компоненти, елементи. Такий різновид концептуальної моделі надає уявлення про об'єкт СІББ, загрози та їхні джерела, взаємозв'язок засобів і дій із забезпечення інформаційної безпеки. На першому етапі розробки структурно-функціональної моделі необхідно розглянути всі елементи та підсистеми СІББ. Результати визначення складових концептуальної моделі подано в табл. 1.

Таблиця 1. Елементи системи

Об'єкти загроз СІББ	Об'єктами загроз ІББ є електронні ресурси, документи; технічні засоби; права й інтереси громадян в інформаційній сфері.
Загрози СІББ	Порушення цілісності, доступності, достовірності, конфіденційності та повноти інформації; порушення прав громадян в інформаційній сфері.
Джерела загроз	Співробітники, користувачі бібліотеки; зловмисники; техногенні та випадкові джерела загроз.
Засоби реалізації загроз	Неправомірний доступ, пошкодження, модифікування, видалення інформації безпосередньо або віддалено.
Напрями забезпечення СІББ	Правовий, організаційний, інженерно-технічний.
Засоби та заходи забезпечення СІББ	Фізичні, програмні, адміністративно-правові.

Змістовне навантаження, а також кількісні та якісні характеристики поданих елементів дещо відрізняються в тій чи іншій бібліотеці, але їх перелік, який відбиває комплексний підхід до формування СІББ, є узагальненим і може змінюватися з розвитком теорії та практики забезпечення інформаційної безпеки й бібліотечної справи.

Для подальшої розробки концептуальної моделі СІББ необхідно визначити зв'язки між підсистемами, проаналізувати службову роль і призначення підсистем стосовно цілого, оцінити взаємозв'язок окремих елементів. На основі визначення інформаційної безпеки бібліотеки як стану захищеності інформаційного середовища, за якого можна забезпечити надійний захист її інформаційних ресурсів і запобігти матеріальній, моральній шкоді користувачам, персоналу й бібліотечному закладу через неправомірне використання та негативний вплив інформації, можна видзначити головний об'єкт СІББ — інформаційне середовище бібліотеки [2]. В аспекті формування СІББ відбувається два види впливу, які умовно можна назвати негативним і позитивним. З одного боку, інформаційне середовище бібліотеки підлягає негативному впливу через реалізацію певними джерелами інформаційних загроз за допомогою різних засобів. З іншого боку, позитивне значення має система заходів з нейтралізації, протидії, локалізації й усунення цих загроз.

Розглянемо елементи СІБ детальніше. Бібліотечні заклади, як являючи собою складова інформаційно-комунікаційної інфраструктури, стикаються з проблемами та ризиками, пов'язаними

із зовнішніми та внутрішніми умовами їхньої діяльності в інформаційному середовищі. Теоретичні та практичні розробки в галузі інформаційної безпеки свідчать про те, що тільки знання про існуючі та потенціальні загрози об'єкту інформаційної безпеки дозволять побудувати адекватну їм систему захисту. Тобто для того, щоб сформувати цілісну та надійну систему інформаційної безпеки бібліотеки, необхідно мати чіткі уявлення щодо загроз і носіїв загроз (джерел) негативного впливу на об'єкти захисту.

У теорії інформаційної безпеки існують декілька підходів щодо класифікації загроз інформаційній безпеці того чи іншого об'єкта. Так, В. Богуш, О. Юдин, В.Ярочкін пропонують виділяти види загроз в залежності від властивостей інформації: конфіденційності (викрадення та втрата інформації), доступності (блокування та знищення), цілісності (модифікація, заперечення, нав'язування) [3; 7]. Інші вчені визначають такі ознаки щодо класифікації загроз інформаційній безпеці: характер виникнення (природні та штучні); ступінь навмисності (випадкові та навмисні); джерело (техногенні, антропогенні, випадкові); ступінь впливу (активні та пасивні) [6]. Аналіз наукових і законодавчих джерел, а також практичної діяльності вітчизняних бібліотек уможливив виділити потенційні загрози їхньої інформаційної безпеки:

- недостатність теоретико-методологічних розробок певної предметної галузі;
- недосконалість інформаційного законодавства України, протиріччя між деякими чинними законодавчими нормами та потребами сучасної інформаційно-бібліотечної сфери. Так, у Законі України «Про авторське право і суміжні права» практично незазначені норми щодо правових засад здійснення такого важливого напряму діяльності бібліотек, як користування електронними ресурсами (створення та доступ до електронних бібліотек, електронна доставка документів, доступ користувачів до Інтернет-ресурсів та електронних книг у бібліотеках);
- модифікація, втрата та пошкодження інформаційних ресурсів бібліотеки;
- здійснення інформаційних атак, зловмисні дії віддалених користувачів;
- негативний вплив вірусів;
- викрадення або пошкодження комп'ютерного устаткування;
- загрози пошкодження інформаційних ресурсів, зумовлені стихійними лихами, техногенними катастрофами;
- навмисне або випадкове пошкодження, викрадення чи видалення інформаційних ресурсів бібліотеки зі сторони зовнішніх джерел загроз;

- неправомірний доступ до персональних даних, які зберігаються та обробляються в бібліотеці.

Потенційні внутрішні загрози інформаційної безпеки публічної бібліотеки — це:

- відсутність або недосконаліть методичного й організаційного забезпечення СІББ;
- надання користувачам бібліотеки недостовірної, неякісної, нерелевантної інформації в процесі інформаційно-бібліографічного обслуговування;
- порушення прав громадян на доступ до інформації, необґрунтоване обмеження доступу користувачів до інформації в бібліотеці;
- порушення прав особистості на захист персональних даних, таємниці бібліотечного-бібліографічного обслуговування;
- навмисні або ненавмисні негативні дії співробітників бібліотеки під час використання електронних ресурсів.

Усі джерела загроз умовно поділено на три групи та зумовлені:

- діями суб'єкта (антропогенні джерела загроз);
- технічними засобами (техногенні джерела загроз);
- стихійними джерелами (випадкові джерела загроз).

Інтенсифікація соціальних інформаційних процесів, розвиток нових інформаційних технологій та внутрішніх технологічних режимів бібліотеки спричинили суттєві зміни в можливостях порушення СІББ. До початку застосування автоматизованих технологій у бібліотечній діяльності головним об'єктом захисту був фонд бібліотеки на паперових носіях. Для реалізації антропогенної загрози інформаційним ресурсам бібліотеки потребувалась, як мінімум, фізична присутність зловмисника або іншого джерела загрози в приміщенні бібліотеки чи біля нього.

Використання технологій Інтернету в інформаційній діяльності бібліотек призвело до виникнення нових засобів реалізації інформаційних загроз, які можуть відбуватись віддалено. Так, порушення контенту сайта, автоматизованої бібліотечно-інформаційної системи, баз даних бібліотеки, може здійснюватися через локальні або глобальні інформаційні мережі, на що слід зважати під час побудови СІББ. Отже, серед основних можливих засобів реалізації загроз інформаційної безпеки бібліотеки можна назвати неправомірний доступ до інформаційних ресурсів, пошкодження, модифікування, видалення інформації безпосередньо або віддалено, недотримання законодавства України під час здійснення інформаційно-бібліографічного обслуговування. Розвиток інформаційних технологій призвів до виникнення нових видів здійснення негативних дій на об'єкт забезпечення інформаційної безпеки — мережевих атак і мережевого шахрайства.

Відповідно до теоретичних розробок спеціалістів у галузі інформаційної безпеки, основними напрямами забезпечення інформаційної безпеки є правовий, організаційний, інженерно-технічний [1; 3; 4; 7]. Застосування всіх цих напрямів є необхідним для формування комплексної СІББ. До правового напряму належать чинні в державі закони, нормативні акти, які регламентують правила використання інформації та відповідальність за їх порушення.

Інженерно-технічний напрям передбачає застосування фізичних, апаратних та програмних засобів. Основним принципом технічного забезпечення інформаційної безпеки бібліотеки є створення та використання комплексу програмно-технічних засобів, який неуможливить здійснення несанкціоноване використання інформаційних ресурсів, а також протидіє можливості знищення технічних засобів, які містять інформаційні ресурси, та безпосередньо інформаційних ресурсів. На сучасному етапі спектр використання технологій захисту інформаційних ресурсів у бібліотеках є дуже широким. Слід відзначити постійне розширення та функціональне вдосконалення, пов'язане з бурхливим розвитком цифрових технологій загалом.

Організаційний напрям містить регламентацію виробничої діяльності на нормативно-правових засадах, забезпечує організацію режиму охорони, роботу з кадрами, документами; регламентує використання технічних засобів й інформаційно-аналітичну діяльність щодо виявлення та аналізу загроз СІББ. Організаційні заходи має чітко планувати, спрямовувати та здійснювати певна організаційна структура чи відповідальні особи.

Кожен з розглянутих напрямів забезпечення інформаційної безпеки бібліотеки передбачає систему заходів та засобів, які реалізуються в комплексі та є взаємодоповнюючими. Серед засобів СІББ виокремлюються такі основні групи: законодавчі, регламентуючі, інструктивно-методичні, організаційно-правові, організаційно-технологічні, морально-етичні, фізичні, програмні, апаратні.

Фізичні, програмні, апаратні засоби в сукупності складають техніко-технологічний інструментарій СІББ.

Вивчення складників СІББ та аналіз зв'язків і розподілення функцій між ними уможливлює розробити структуру концептуальної моделі СІББ (рис. 1)

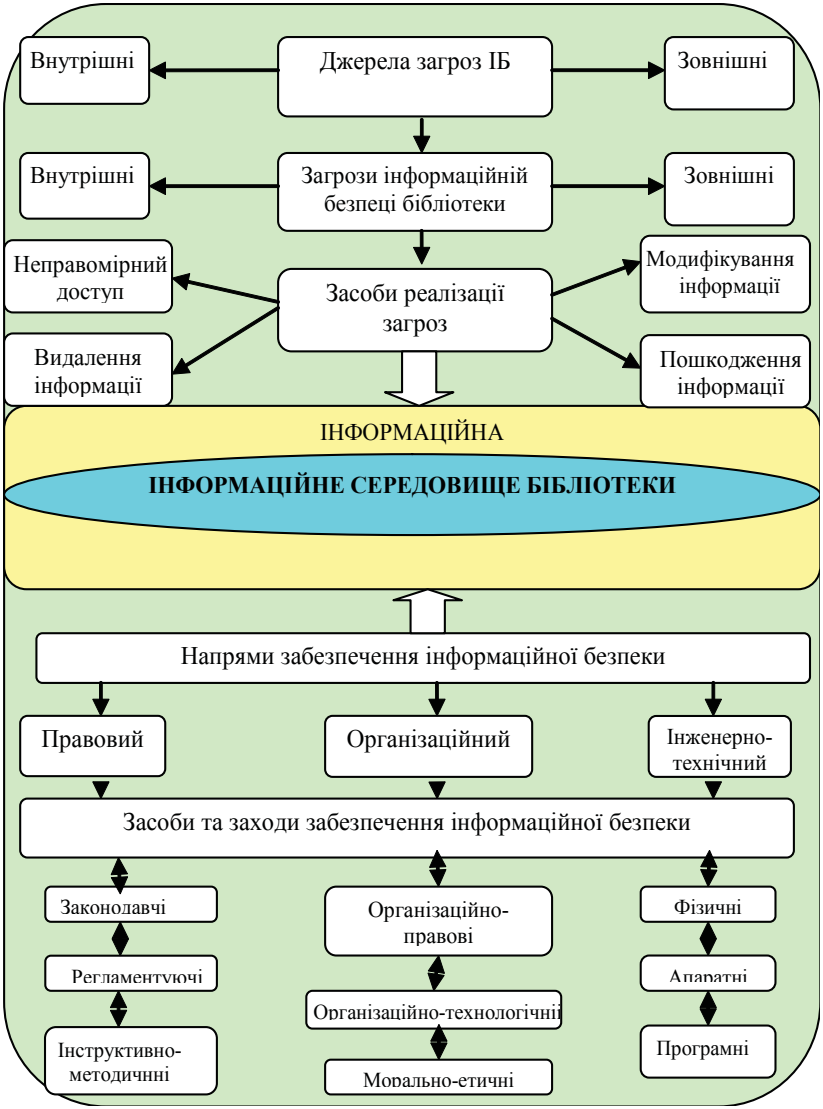

Рис. 1 Концептуальна модель системи інформаційної безпеки бібліотеки

Таким чином, забезпечення інформаційної безпеки бібліотеки є проблемою високої складності та потребує комплексного підходу, тому для ефективного функціонування СІББ сукупність зазначених організаційно-технологічних та організаційно-правових

заходів слід поєднати в систему управління інформаційною безпекою.

Запропонована концептуальна модель СІББ містить основні позиції, на які слід зважати під час забезпечення інформаційної безпеки, та дозволяє збільшити ефективність процесів і результатів управління бібліотечно-інформаційною діяльністю в цій галузі. Необхідність подальшої розробки проблеми безпеки інформаційного середовища вітчизняних бібліотек зумовлює нагальність досліджень, пов'язаних із науковим обґрунтуванням динаміки СІББ в аспекті розвитку системи соціальних комунікацій; вивченням диференціації загроз інформаційної безпеки відповідно до виду та типу бібліотеки; аналізом перспективних форм соціальної взаємодії з питань додержання безпеки інформаційного середовища.

Список літератури

1. Асанович В. Я. Информационная безопасность: анализ и прогноз информационного воздействия / В. Я. Асанович, Г. Г. Маньшин. — Мн. : Амалфея, 2006. — 204 с.
2. Бобришева О. В. Бібліотека як суб'єкт забезпечення інформаційної безпеки / О. В. Бобришева // Бібліотекознавство. Документознавство. Інформологія. — 2011. — № 3. — С. 24–29.
3. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. — К. : «МК — Прес», 2005. — 432 с.
4. Кормич Б. А. Інформаційна безпека: організаційно-правові основи / Б. А. Кормич. — К. : Кондор, 2003. — 384 с.
5. Плотинский Ю. М. Модели социальных процессов : учеб. пособ. для вузов / Ю. М. Плотинский. — изд. 2-е, перераб. и доп. — М. : Логос, 2001. — 286 с.
6. Цирлов В. Л. Основы информационной безопасности автоматизированных систем : краткий курс / В. Л. Цирлов. — Ростов-на-Дону, 2008. — 173 с.
7. Ярочкин В. И. Информационная безопасность : [учебник для вузов] / Ярочкин В. И. — [2-е изд]. — М. : Академический Проект; Гаудеамус, 2004. — 544 с.
8. ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management: international standard. — Geneva, 2005. — 108 p.
9. ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary: international standard. — Geneva, 2009. — 19 p.
10. Newby G. Information security for libraries / Newby G // Proceedings of 2000 information resources management association international technology management in the 21th century. — Hershey, PA : IGI Publishing, 2000. — P. 558–560.

Надійшла до редколегії 19.02.2013 р.