ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВСЬКОЇ СФЕРИ В УКРАЇНІ
INFORMATION SECURITY OF THE BANKING SECTOR IN UKRAINE

УДК 336.71:004.056.5
DOI https://doi.org/10.32782/pma2663-5240-2024.40.32

Новицький В.А.
аспірант кафедри
публічного управління та
землевпорядкування,
Класичний приватний університет
ORCID ID: 0009-0007-3687-3232

Питання забезпечення інформаційної безпеки в глобальному світі не оминуло й Україну. Особливо після початку повномасштабної війни між Росією та Україною наша країна зазнає кібератак на інформаційну інфраструктуру країни (державне програмне забезпечення, державні сайти, інформаційно-технічне забезпечення стратегічних державних об'єктів, банківські установи), всебічного впливу антиукраїнської інформації, розповсюдження дезінформації, дезінформації, сепаратизму, розбрату та насильства. Країна постійно потерпає від поширення ідеології. Ворог використовує різноманітні методи впливу на українців, підриває засади національної безпеки, порушує культурну самобутність українського народу, порушує дипломатичні відносини та міжнародні угоди між Україною та її стратегічними партнерами, провокує етнічні та релігійні конфлікти в країні та, зрештою, прагне підірвати конституційний лад і намагається порушити територіальну цілісність держави.

Сьогодні не тільки вітчизняні медіаресурси, а й навіть відомі міжнародні видання з різних причин часто однобічно або неповно висвітлюють інформацію та події, що відбуваються в Україні, порушуючи цілісність країни. Український народ дедалі частіше зазнає інформаційно-психологічного тиску в контексті гібридної війни. З огляду на викладене вище, Україні необхідно розробити надійні механізми захисту конфіденційності, доступності та цілісності інформації, що унеможливлять порушення законних прав та інтересів громадян, приватних і громадських організацій та держави загалом.

У даній статті висвітлено особливості забезпечення інформаційної безпеки в банківській системі України, проаналізовано чинники, що впливають на цілісність, доступність і конфіденційність інформації. Автор звертає увагу читача на необхідність розвитку інформаційної культури суспільства. Ця культура дасть змогу адекватно протистояти загрозам у контексті гібридної війни, що включає повномасштабні та водночас потужні інформаційні елементи, з якими стикається сучасна Україна.

Ключові слова: *банківська система; інформаційна безпека; загроза; ризик; безпека інформаційних ресурсів; безпека інформаційної інфраструктури; безпека інформаційного сектору.*

The issue of ensuring information security in the global world did not escape Ukraine either. Especially after the start of a full-scale war between Russia and Ukraine, our country is subject to cyber attacks on the country's information infrastructure (state software, state websites, information and technical support of strategic state objects, and banking institutions), the comprehensive influence of anti-Ukrainian information, disinformation, misinformation, separatism, discord, and violence. The country constantly suffers from the spread of ideology. The enemy uses various methods of influencing Ukrainians, undermines the foundations of national security, violates the cultural identity of the Ukrainian people, violates diplomatic relations and international agreements between Ukraine and its strategic partners, provokes ethnic and religious conflicts in the country, and, ultimately, seeks to undermine the constitutional order and tries to violate the territorial integrity of the state.

Today, not only domestic media resources but also well-known international publications, for various reasons, often one-sidedly or incompletely cover information and events taking place in Ukraine, violating the integrity of the country. The Ukrainian people are increasingly exposed to informational and psychological pressure in the context of hybrid warfare. Given the above, Ukraine needs to develop reliable mechanisms for protecting the confidentiality, availability, and integrity of information, which will make it impossible to violate the legal rights and interests of citizens, private and public organizations, and the state in general.

This article highlights the peculiarities of ensuring information security in the banking system of Ukraine and analyzes the factors affecting the integrity, availability, and confidentiality of information. The author draws the reader's attention to the need to develop the information culture of society. This culture will make it possible to adequately resist threats in the context of hybrid warfare, which includes full-scale and at the same time powerful informational elements that modern Ukraine faces.

Key words: *banking system; informational security; threat; risk; security of information resources; information infrastructure security; security of the information sector.*

Постановка проблеми. Розбудова України як правової держави призведе до реформування всіх сфер життя суспільства, зокрема й правовідносин в економічній та фінансовій сферах, які значною мірою залежать від ефективної банківської діяльності.

З огляду на те, що банківська система сучасної держави не існує сама по собі, а тісно взаємопов'язана з банківськими системами інших держав і міжнародних банківських організацій, проблема забезпечення надійності, безпеки та стабільності банківської діяльності виходить далеко за рамки суто внутрішнього регулювання.

Аналіз останніх досліджень та публікацій. У роботах вітчизняних і зарубіжних учених та експертів представлено низку досліджень, присвячених інформаційній безпеці банківських установ, а саме: В. М. Ахрамович, К. І. Бєлоусова, В. М. Богуш, М. Ф. Богдаренко, А. М. Гребенюк, М. О. Диба, В. В. Домарєв, А. І. Марущак та багато інших. Проте для роз-

роблення ефективної системи забезпечення інформаційної безпеки в банках необхідні подальші дослідження.

Метою роботи виступає вивчення теоретичних засад інформаційної безпеки установ банківської сфери.

Виклад основного матеріалу. Сьогодні в українських банках створено певні системи інформаційної безпеки. Це можна розглядати як сталий стан життя та гарантію реалізації основних інтересів і пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих чинників, незалежно від умов діяльності банку. Основним критерієм ефективності банківської безпеки є стабільність фінансово-економічного становища банку.

Мета банківських гарантій – унеможливити виникнення у банку збитків або упущеної вигоди, забезпечити ефективність діяльності та якість угод і контрактів.

Нині інвестиції в інформаційну безпеку не здійснюються. Основні види банківської безпеки можна виділити, якщо врахувати, що банківська безпека – це багатогранна система, яка захищає інтереси банків [2].

Інформаційна безпека у вітчизняних банках не є традиційною статтею витрат, на відміну від зарубіжних. Не всі керівники розуміють важливість механізмів інформаційної безпеки. Проте ця галузь динамічно розвивається, і сьогодні передбачено ефективні механізми та заходи щодо захисту й охорони виробничої діяльності банків. У період економічної кризи керівники компаній і банків змушені скорочувати витрати, і в таких ситуаціях насамперед страждає бюджет, виділений на інформаційну безпеку. Порушення цілісності критично важливої інформації може призвести до непередбачуваних наслідків, як-от втрата важливих програм або комерційних секретів. Під час економічного спаду кількість прогнозованих інцидентів, пов'язаних з інформаційною безпекою, продовжує зростати, роблячи компанії та банки більш уразливими [6, с. 9-25].

Стаття 54 Закону України «Про банки і банківську діяльність» встановлює засади дій щодо захисту банківської власності. Згідно з положеннями статті, банки мають право забезпечувати захист інформації, коштів та майна банку шляхом створення відповідних систем безпеки та охоронних послуг відповідно до законодавства України та нормативних актів Національного банку України. Ці положення Закону надають банкам відповідні привілеї, на відміну від інших суб'єктів, на яких вони не поширюються. Щодо останніх, то статті 27, 28, 29 і 42 Конституції України гарантують право на життя, здоров'я, повагу до особи, недоторканність місця проживання та підприємницької діяльності. На жаль, захист підприємницької діяльності не гарантовано жодним законодавчим актом [7].

Режим захисту банківських даних ґрунтується на таких законодавчих актах:

– Закон України «Про банки і банківську діяльність» (стаття 52 «Банківська таємниця»);

– Закон України «Про підприємства України» (стаття ЗО «Комерційна таємниця підприємств»);

– Закон України «Про інформацію» (стаття ЗО «Інформація обмеженого доступу»).

З юридичної точки зору режим захисту інформації обмеженого доступу є найбільш досконалим. З цією метою Закон дає чітке визначення банківської таємниці (стаття 52 Закону України «Про банки і банківську діяльність»). Згідно із Законом, до банківської таємниці відносяться відомості про операції, рахунки і вклади клієнтів банку та кореспондентів (контрагентів). Вирішення цієї проблеми має бути комплексним:

– повний програмно-апаратний комплекс,

– програми безпеки,

– включає в себе бесіди і роботу зі співробітниками.

В українських банках захист інформації здебільшого ґрунтується на використанні дешевих продуктів і нелегальному застосуванні неоригінального програмного забезпечення. Такий підхід не захищає діяльність банку від внутрішніх і зовнішніх загроз. Відповідні корпоративні стандарти безпеки існують в Україні в телекомунікаціях, банках і компаніях з міжнародними стандартами управління [4].

Оскільки цей сектор бізнесу стає найважливішим ресурсом, а інформаційні технології – невід'ємною частиною кожного процесу, відсутність подібних систем безпеки – мабуть, найголовніший ризик для бізнесу.

Необхідний комплексний підхід до інформаційної безпеки. Інформаційна безпека має розглядатися як важлива і невід'ємна частина загальної безпеки. У розробленні концепції інформаційної безпеки обов'язково має брати участь відділ безпеки банку. Ця концепція повинна включати не тільки заходи, пов'язані з інформаційними технологіями (наприклад, захист від шифрування, програмні засоби управління правами користувачів, ідентифікації та автентифікації, міжмережеві екрани для захисту мережевих входів і виходів), а й суворі процедури контролю фізичного доступу до автоматизованих банківських систем, банківської системи та необхідно також передбачити адміністративні й технічні заходи, як-от засоби синхронізації й обміну даними між модулем

управління безпекою й системою безпеки, а також засоби для забезпечення безпечного доступу до системи безпеки [9, с. 102-104].

Надійність та ефективність банківської діяльності забезпечуються за рахунок реалізації відповідних вимог до систем безпеки банків (безперервність, планування, конкретність, активність, універсальність і комплексність). Сили безпеки керуються у своїй діяльності відповідними принципами, заснованими на принципі законності.

Стрімка інформатизація та розвиток глобальних інформаційно-комунікаційних мереж не тільки автоматизують звичні банківські процеси, а й надають постійні можливості для створення нових банківських продуктів (послуг) (сьогодні це SMS-банкінг, інтернет-банкінг та web money banking).

З огляду на те, що банківські операції значною мірою залежать від надійності використовуваних інформаційних технологій, забезпечення інформаційної безпеки стає одним з основоположних принципів банківської системи в цілому. Одним з основних напрямів забезпечення інформаційної безпеки в банківських установах є захист банківської таємниці [11].

Структура інформаційної безпеки в банківських установах включає такі ключові елементи

– Безпека інформаційних ресурсів,

– Безпека інформаційної інфраструктури,

– Безпека інформаційного сектору.

Інформаційні ресурси банківської установи – це взаємопов'язана, упорядкована, організована та зафіксована на матеріальному носії інформація, що належить банківській установі. Тож безпека інформаційних ресурсів – це захист такої інформації від несанкціонованого поширення, використання та порушення конфіденційності (секретності).

Безпека інформаційної інфраструктури – це стан захищеності електронно-обчислювальних машин, систем, комп'ютерних мереж і телекомунікаційних мереж банківських установ, що гарантує цілісність і доступність оброблюваної (збереженої або циркулюючої) в них інформації.

Безпека інформаційного сектору банківської установи ґрунтується на контрольованості переважно несистематизованого потоку інформації, що її публікують різні учасники інформаційних відносин, включно з мовними компаніями, друкованими ЗМІ, інтернет-виданнями, конкурентами, органами державної влади та місцевого самоврядування [10].

Інформаційна безпека будь-якої організації ґрунтується на системі заходів безпеки, реалізованих відповідно до її вимог до безпеки. Основними джерелами інформації про вимоги до інформаційної безпеки організації є:

1) результати оцінювання ризиків організації з урахуванням загальної стратегії та цілей бізнесу (під час оцінювання ризиків виявляють загрози ресурсам СУІБ, оцінюють уразливість і ймовірність подій, визначають величину потенційних наслідків);

2) правові вимоги, визначені законодавством, контрактами та угодами з партнерами організації; і

3) власний набір принципів, цілей і бізнес-вимог до обробки інформації, розроблених організацією для підтримки своїх функцій [15].

З упровадження систем управління інформаційною безпекою та методології оцінки ризиків відповідно до стандартів Національного банку України як джерела вимог до інформаційної безпеки зазначено такі:

– Законодавство України,

– Нормативні акти Національного банку України,

– Вимоги до систем платежів і грошових переказів,

– Внутрішні нормативні документи банків,

– Угоди та договірні умови з третіми особами.

Важливо зазначити, що вимоги до інформаційної безпеки платіжних систем та систем грошових переказів можуть відрізнятися від вимог Національного банку України, оскільки вони встановлюються розрахунковою організацією платіжної системи (електронні платіжні системи (ЕПС), де розрахунковою організацією є Національний банк України, і національні масові Електронна платіжна система (ЕПС), розрахунковою організацією якої є Національний банк України, і національна масова електронна платіжна система (НМЕПС) виключені) [17].

Особливу увагу слід приділяти умовам угод і договорів із третіми сторонами: відповідно до пункту 6.2 Стандарту НБУ 65.1 ISMS 2.0:2010 безпеку інформації та засобів обробки інформації банку не має бути поставлено під загрозу внаслідок упровадження продуктів або послуг зовнішніх сторін. За наявності ділової необхідності в роботі із зовнішніми сторонами, яким може знадобитися доступ до інформації або засобів оброблення інформації банку, а також для одержання або надання продуктів або послуг від зовнішніх сторін, банк повинен провести оцінку ризиків для визначення вимог безпеки та наслідків порушення безпеки. провести оцінку ризиків. Заходи безпеки мають бути узгоджені та визначені в договорах із зовнішніми сторонами. Ці питання

мають розглядатися не тільки в договорах на надання послуг клієнтам банку (наприклад, банківські системи для клієнтів, інтернет-банкінг, мобільний банкінг), а й під час отримання послуг від зовнішніх сторін (наприклад, розробка та супровід програмного забезпечення, придбання та обслуговування обладнання, надання послуг зв'язку), також беруться до уваги [19].

Аналіз вимог з перерахованих вище джерел допомагає правильно визначити цілі та заходи безпеки СУІБ, здатні знизити ризики і вразливості банківської діяльності, з урахуванням специфіки банківських операцій.

Уразливості, на які можуть негативно вплинути загрози інформаційній безпеці банку, розглядаються на таких рівнях

– Банк загалом,
– Процеси та процедури,
– Системи управління,
– Персонал,
– Фізичне середовище,
– Програмне забезпечення, апаратні системи, обладнання тощо,
– Залежність від зовнішніх організацій.

Водночас неправильні або неефективні заходи безпеки – це вид уразливості, який знижує рівень безпеки банку загалом і кожного бізнес-процесу/банківського продукту окремо [12].

Оцінювання інформаційної безпеки банківської установи проводиться з погляду основних сервісів інформаційної безпеки:

Конфіденційність – характеристика інформації, що означає, що інформація не може бути отримана неавторизованими користувачами та/або процесами;

цілісність системи – властивість системи, яка означає, що жоден компонент системи не може бути видалений, змінений або доданий у порушення політики безпеки;

доступність – означає, що відповідним чином авторизовані користувачі та/або процеси можуть використовувати ресурс у потрібній користувачеві формі, у потрібному користувачеві місці та в потрібний користувачеві час, не чекаючи довше за вказаний (номінальний) термін, згідно з правилами, встановленими політикою безпеки; та характеристика системного ресурсу, що означає, що його можна використовувати у тій формі, у тому місці й у той час, коли це необхідно користувачеві; і

підзвітність – здатність реєструвати дії користувачів і процесів, пасивне використання об'єктів і чітко встановлювати ідентифікатори користувачів і процесів, залучених до події, з метою запобігання порушенням політики безпеки та/або забезпечення підзвітності за певні дії [1, с. 139-143].

Вплив основних сервісів інформаційної безпеки оцінюється для кожного бізнес-процесу/банківського продукту, програмно-апаратного комплексу банку. Слід зазначити, що одні й ті самі ризики від втрати основних сервісів інформаційної безпеки можуть бути виявлені для різних бізнес-процесів/банківських продуктів. Це свідчить про певний розрив у забезпеченні інформаційної безпеки в банку. У цьому випадку необхідно вжити відповідних заходів щодо зниження виявлених ризиків інформаційної безпеки для всіх бізнес-процесів/банківських продуктів банку.

Основними характеристиками інформаційної безпеки в банках є такі:

– Інформаційна безпека охоплює інформацію про персонал (керівництво, відповідальні особи та співробітники); інформацію про технології, які використовує банк; інформацію про інформаційні ресурси (інформація про діяльність і фінансовий стан клієнтів, що стає відома банку в процесі обслуговування, інформація про всі операції банку та фінансову звітність, інформація в конфіденційній електронній мережі);

– Основними завданнями системи інформаційної безпеки є забезпечення стабільного функціонування банку, запобігання загрозам його безпеці, захист від неправомірного посягання, розголошення, втрати, витоку, викривлення та знищення службової інформації, переривання роботи технічних засобів і забезпечення виробничої діяльності з використанням інформаційних технологій;

– Основні завдання, розв'язувані інформаційною безпекою банку, включають забезпечення доступу керівництва банку до чутливої для ринку інформації, запобігання витоку або знищення конфіденційної банківської інформації, а також забезпечення розповсюдження «чутливої» інформації, корисної для банку, у зовнішнє середовище [5, с. 53].

У центрі нашої уваги перебувають питання запобігання, виявлення та мінімізації загроз інформаційній безпеці банку. По суті, це сукупність внутрішніх і зовнішніх умов, спрямованих на порушення нормального функціонування інформаційної інфраструктури банку, які можуть завдати шкоди інтересам власників, працівників і клієнтів банку.

За результатами досліджень вчених економістів, як вітчизняних, так і зарубіжних, можна виділити кілька видів загроз інформаційній безпеці банківських установ. Серед них: незаконне збирання та використання інформації; порушення технології та правил обробки

інформації; впровадження компонентів у апаратні та програмні засоби, які не передбачені документацією; розроблення та поширення програм, які порушують нормальне функціонування інформаційно-телекомунікаційних систем банківських установ; несанкціонований доступ до інформації в банківських установах та їхніх базах даних; перехоплення інформації, що циркулює в засобах зв'язку та обчислювальної техніки, за допомогою технічних засобів негласного зняття інформації, несанкціонованого доступу та навмисних технічних впливів на них під час обробки та зберігання; підслуховування з використанням технічних засобів конфіденційних переговорів, що ведуться в службових приміщеннях [3, с. 37, 14, с. 22].

Усі загрози можна поділити на такі категорії:

1) випадкові загрози: помилки або події, які не залежать від людини (спричинені природними явищами або діяльністю людини);

2) навмисні загрози: можуть бути здійснені учасниками процесу обробки інформації (копіювання або крадіжка програмного забезпечення, несанкціоноване введення даних, зміна або знищення даних на магнітних носіях, крадіжка інформації, неправомірне використання комп'ютерних ресурсів, неправомірне використання автоматизованих банківських систем, несанкціонований доступ до конфіденційної інформації, (знищення інформації);

3) спотворення інформації: порушення цілісності, включно зі зміною змісту та часткове знищення [13].

Цікавими є результати опитування Спецслужби про фактори, що створюють умови для витоку інформації:

– надмірна балакучість співробітників банку (32%);

– бажання співробітників банку заробити гроші будь-яким способом і за будь-яку ціну (24%);

– відсутність системи заходів, спрямованих на захист інформації (14%);

– практика обміну співробітниками банку новинами, чутками та інформацією один з одним (12%); і

– нерегульоване використання інформаційних систем (10%);

– наявність передумов для виникнення конфліктів між співробітниками банку (8%) [11, с. 43].

Класифікація загроз інформаційної безпеки на безліч типів практично повністю повторює існуючу класифікацію ризиків інформаційної безпеки, яку можна знайти на сайті. Це ще раз підтверджує той факт, що загрози є варіантами (або стадіями) виникнення ризиків [16, с. 133-145] Автори повністю підтримують точку зору [16, с. 133-145] щодо взаємозв'язку цих категорій:

– Загроза – це такий розвиток подій або дій (бездіяльності), який порушує нормальне функціонування підприємства, у тому числі завдає йому певної шкоди, і створює або збільшує ймовірність того, що воно не досягне своїх цілей;

– Ризик – це ведення бізнесу в невизначених обставинах або сама невизначеність ситуації чи результату бізнесу.

Таким чином, загроза – це відомий несприятливий сценарій, який почав розгортатися небажаним чином і, отже, виходить за рамки звичайного поняття невизначеності в умовах бізнесу. Оскільки фактори ризику існують, ними необхідно розумно управляти, ретельно й адекватно оцінювати структуру та ступінь ризику, а також докладати зусиль для зниження рівня ризику до прийнятного [18, с. 134-139]. Використовуючи дослідження природи інформаційного ризику в банківській діяльності, проведене авторами статті «Інформаційні ризики в банківській діяльності» [8, с. 29]. Тут акцент робиться на визначенні поняття та специфічних характеристик цих ризиків.

Заходи безпеки банків набувають форми охоронного, структурного, інформаційного та аналітичного забезпечення їхньої діяльності. Ця форма забезпечення безпеки в практичній діяльності банків є найбільш типовою для банківських операцій і прийнята практично всіма банками світу. Досягнення цілей безпеки банку забезпечується вирішенням таких завдань.

– Попередження і стримування злочинних і кримінальних посягань на майно, персонал та імідж банку;

– своєчасне виявлення реальних і потенційних загроз банку та вжиття заходів щодо їх нейтралізації; і

– своєчасне виявлення змін і негативних тенденцій у сферах діяльності банку, його інтересів та інформації, що заслуговує на увагу, і забезпечення своєчасного реагування організаційних елементів банку;

– виявлення і формування умов, що сприяють реалізації інтересів банку;

– навчання та підготовка персоналу банку з питань безпеки

– зниження негативних наслідків дій конкурентів і злочинців, спрямованих на підрив безпеки банку; і

– збереження та ефективне використання фінансових, матеріальних та інформаційних ресурсів банку.

Висновок. Отже, інформаційна безпека дає змогу зберігати й ефективно використовувати фінансові, матеріальні та інформаційні

ресурси банку, вчасно виявляти й нейтралізувати реальні та потенційні загрози, а також створювати умови для реалізації стратегічних інтересів банку.

ЛІТЕРАТУРА:

1. Аніщук В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського Національного Університету.* Серія ПРАВО. Випуск 77 : частина 2. 2023. С. 139–143.
2. Ахрамович В. М. Інформаційна безпека : навч. посіб. К. : ДП «Інформ.– аналіт. Агенство», 2009. 276 с.
3. Бєлоусова К. І. Забезпечення інформаційної безпеки – реалізація стратегії банківської установи. *Науковий вісник ДУІКТ*. 2010. С.33–38.
4. Богуш В. М., Юдін О. К. Інформаційна безпека держави : навчальний посібник. К. : «МК-Прес», 2005. 432 с.
5. Бодюл Є. М. Інформаційна безпека банку. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж : тези доповідей *Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року).* Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми : ДВНЗ «УАБС НБУ», 2010. С.53–55.
6. Бондаренко М. Ф. Визначення та обґрунтування суті політики інформаційної безпеки. *Радиотехника*. 2003. № 134. С. 9–25.
7. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. унт. внутріш. справ, 2020. 144 с.
8. Диба М. О. Інформаційні ризики в банківській діяльності. *Вісник НБУ.* 2007. С.28–35.
9. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою. *Вісник Державного університету інформаційно-комунікаційних технологій*. 2012. Т. 10, № 2. С. 102–104.
10. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом : навчальний посібник. К. : НАУ, 2006. 108 с.
11. Зубок М. І. Безпека банківської діяльності : навч. посібник. К. : КНЕУ, 2002. 190 с.
12. Кобозева А. А., Мачалін І. О., Хорошко В. О. Аналіз захищеності інформаційних систем : підручник. К. ДУІКТ, 2010. 316 с.
13. Козаченко І. П. Загальні принципи захисту банківської комп'ютерної інформації. *Центр дослідження проблем комп'ютерної злочинності.* Електронний ресурс. Режим доступу: http://www.crime-research.ru/library/Koz_gol.htm
14. Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж : тези доповідей *Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року).* Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми : ДВНЗ «УАБС НБУ», 2010. С.21–24.
15. Лужецький В. А., Войтович О. П., Дудатьєв А. В. Інформаційна безпека : навчальний посібник. Вінниця : УНІВАР-СУМ-Вінниця, 2009. 240 с.
16. Радевич Н. Інформаційна безпека України в контексті Євроінтеграції. *Міжнародний науковий вісник*. No1-2 (23-24). 2021. С. 133–145.
17. Самохвалов Ю. Я., Темніков В. О., Хорошко В. О. Організаційно-технічне забезпечення захисту інформації. К. : Видавництво НАУ, 2002. 208 с.
18. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету.* Серія Право. Випуск 78 : Частина 2. 2023. С. 134–139.
19. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення : підруч. К. : НАУ, 2011. 640 с.