УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

МЕТОДИКА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В БАНКІВСЬКИХ УСТАНОВАХ ЗА ДОПОМОГОЮ СУІБ «МАТРИЦЯ»

Дмитро Домарєв, Валерій Домарєв

Національний авіаційний університет, Україна

ДОМАРЄВ Дмитро Валерійович

Рік та місце народження: 1989, м. Київ, Україна.
Освіта: вища, Національний авіаційний університет.
Посада: аспірант.
Наукові інтереси: системний підхід до інформаційної безпеки, управління інформаційною безпекою, аналіз захищеності інформаційних систем.
Публікації: 10 з питань інформаційної безпеки.
E-mail: dimavsesvit@yahoo.com.

ДОМАРЄВ Валерій Валентинович, к.т.н., доц.

Рік та місце народження: 1957, м. Пружани, Білорусь.
Освіта: вища, Національна академія оборони України.
Посада: незалежний експерт з питань інформаційної безпеки.
Наукові інтереси: системний підхід до інформаційної безпеки, управління інформаційною безпекою, оцінювання ризиків інформаційної безпеки.
Публікації: понад 40 з питань безпеки інформаційних технологій.
E-mail: domarev@ukr.net.

Анотація: *Обґрунтована актуальність питань управління інформаційною безпекою. Теоретичною основою пропонованої методики є системний підхід до інформаційної безпеки. Для практичної реалізації пропонованої методики застосовано систему управління інформаційною безпекою «Матриця». Наведені процедури формування нормативної бази щодо інформації з обмеженим доступом, опису критичних бізнес-процесів та програмно-технічних комплексів, які забезпечують їх функціонування, опису організаційної структури банку, яку охоплює СУІБ, призначення відповідальних осіб за впровадження СУІБ, оцінювання ризиків інформаційної безпеки банківської установи, створення плану відновлення у разі надзвичайних обставин. Зроблено висновки про застосовність пропонованої методики в управлінні інформаційною безпекою банківських установ.*

Ключові слова: *управління інформаційною безпекою, СУІБ «Матриця», системний підхід до ІБ, система управління інформаційною безпекою, формування нормативних документів, ГСТУ СУІБ, ISO 27000, оцінювання ризиків ІБ.*

Вступ

Актуальність пропонованої методики виходить з вимог Галузевих стандартів Національного банку України (НБУ) [3, 4] щодо обов'язкового впровадження систем управління інформаційною безпекою (СУІБ) в усіх банківських установах держави.

Метою розробки пропонованої методики є полегшення впровадження і застосування СУІБ в банківських установах на прикладі розробленої авторами СУІБ «Матриця».

Задачею, яку має вирішити пропонована методика, є конкретизоване роз'яснення процесу виконання тих вимог стандартів ГСТУ СУІБ, котрі викладені переважно в загальній формі. Кожний розділ даної статті присвяченій окремій вимозі.

Автори провели дослідження [2], в якому розглянули теоретичні та практичні питання впровадження вимог галузевих стандартів України

та міжнародних стандартів управління інформаційною безпекою (ІБ) [7, 8] на прикладі банківських інформаційних технологій. Пропонована методика є результатом згаданого дослідження.

Методичним інструментом впровадження вимог стандартів обрано системний підхід до ІБ [1], а засобом – СУІБ «Матриця» [6]. При проведенні даного дослідження, для більш точного охоплення банківських процесів, складові класичної Матриці системного підходу до ІБ було змінено наступним чином.

1. Основу №3 «Заходи» замінено на «Політика»;

2. Напрямки повністю замінені на такі:

2.1. Система електронних платежів НБУ;

2.2. Карткові платіжні системи;

2.3. Інформаційні системи банку;

2.4. Системи електронної комерції ;

2.5. Комунікації;

3. Визначення деяких етапів конкретизовані:

3.1. Етап №1 «Визначення інформації, що підлягає захисту» перейменовано у «Визначення активів, що підлягають захисту»;

3.2. Етап №4 «Визначення вимог до СЗІ» перейменовано у «Формування вимог до СУІБ»;

3.3. Етап №6 «Впровадження і використання обраних заходів і засобів» перейменовано у «Впровадження, навчання та використання СУІБ»;

3.4. Етап №7 «Контроль цілісності і управління захистом» перейменовано у «Контроль та оцінка ефективності СУІБ»;

Адаптована Матриця системного підходу до ІБ банківських установ зображена на рис. 1. Всі процеси, що описані нижче, засновані на елементах наведеної Матриці.

Формування нормативної бази щодо інформації з обмеженим доступом

Процес визначення відомостей, що віднесено до банківської таємниці, та формування відповідних нормативних документів з дотриманням системного підходу до ІБ зображено на рис. 2.

Формування нормативної бази щодо інформації з обмеженим доступом в СУІБ «Матриця» відбувається наступним чином.

1. Доповнити список активів категоріями інформації з обмеженим доступом, а також сформувати список співробітників (підрозділів) банку.

<<< ЕТАПИ	НАПРЯМКИ >>>	010				020				030				040				050			
		Система електронних платежів НБУ				Каркові платіжні системи				Інформаційні системи банку (АБС)				Системи електронної комерції				Комунікації			
	ОСНОВИ >>>	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби	База	Структура	Політика	Засоби
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Визначення активів, що підлягають захисту	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Виявлення загроз і каналів витоку	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Оцінка ризиків	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Формування вимог до СУІБ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Визначення засобів та заходів ІБ	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Впровадження, навчання та використання СУІБ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль та оцінка ефективності СУІБ	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис. 1. Матриця системного підходу до ІБ для банківських установ

2. Ввести документи, що стосуються обробки інформації з обмеженим доступом в модуль «Знання», і визначити як мінімум відповідального та активи для кожного розділу кожного документа.

3. Відкрити зведену таблицю «Активи за відповідальними» і вибрати активи, що відповідають інформації з обмеженим доступом. Отримане відображення використовувати для формування зобов'язань працівників щодо збереження інформації з обмеженим доступом.

4. Скомпонувати документ для певного активу за допомогою форм «Умови відбору» та «Формування документів / звітів».

5. Отриманий документ (рис. 3) можна використовувати як положення щодо спеціального діловодства для документів, які містять інформацію з обмеженим доступом.

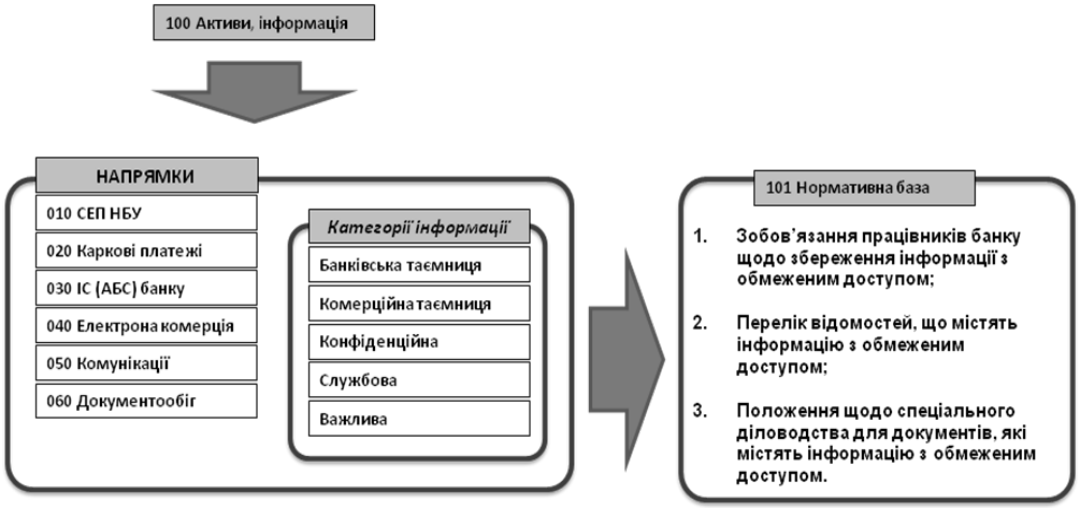


Рис. 2. Процес визначення відомостей, що віднесено до банківської таємниці, та формування відповідних нормативних документів

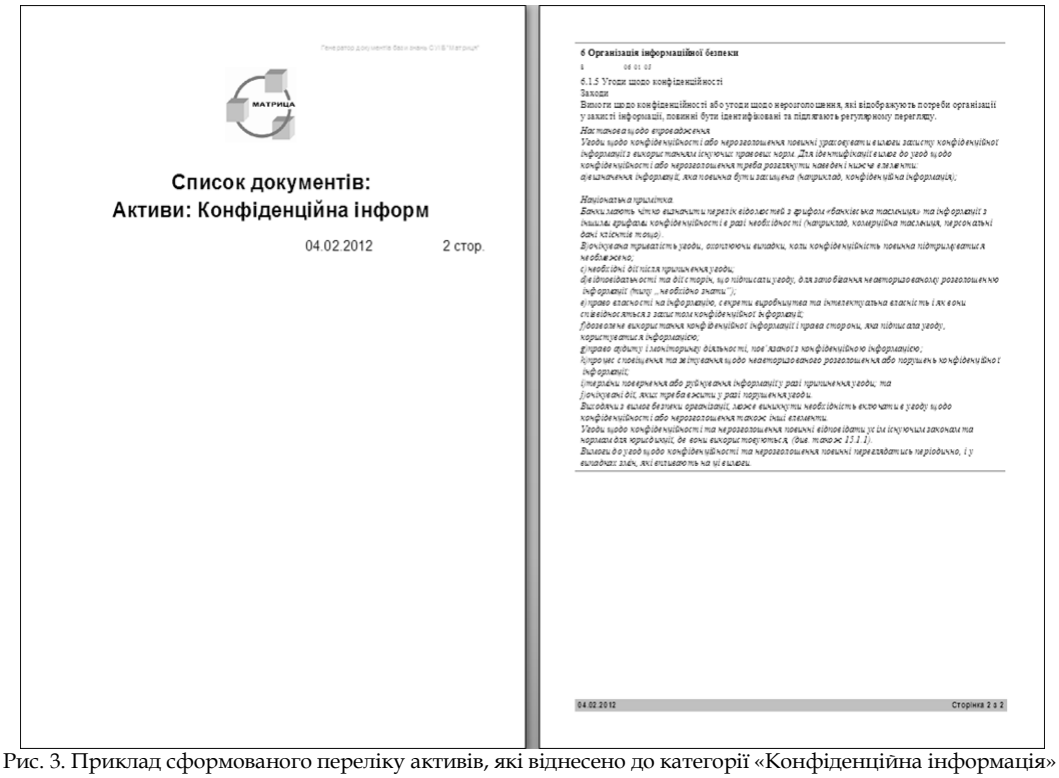


Рис. 3. Приклад сформованого переліку активів, які віднесено до категорії «Конфіденційна інформація»

Опис критичних бізнес-процесів та програмно-технічних комплексів, які забезпечують їх функціонування

Процес опису критичних бізнес-процесів та формування відповідних документів з дотриманням системного підходу до ІБ зображено на рис. 4.

Опис критичних бізнес-процесів в СУІБ «Матриця» відбувається наступним чином:

1. Заповнити список напрямків діяльності банку назвами критичних бізнес-процесів, головних продуктів (послуг) та найважливіших комплексів.

2. Заповнити список великих об'єктів, що задіяні в діяльності банку. Зазвичай один об'єкт може бути пов'язаний з кількома напрямками.

3. Доповнити список активів докладним переліком систем та програмно-технічних комплексів, що задіяні у критичних бізнес-процесах банку.

4. За допомогою модуля «Знання» призначити кожному розділу кожного документа (кожному запису) напрямок, об'єкт та актив.

5. Відкрити зведену таблицю «Активи за відповідальними», що наочно ілюструє структуру критичних бізнес-процесів, головних продуктів (послуг) та найважливіших програмно-апаратних комплексів банку (рис. 5).

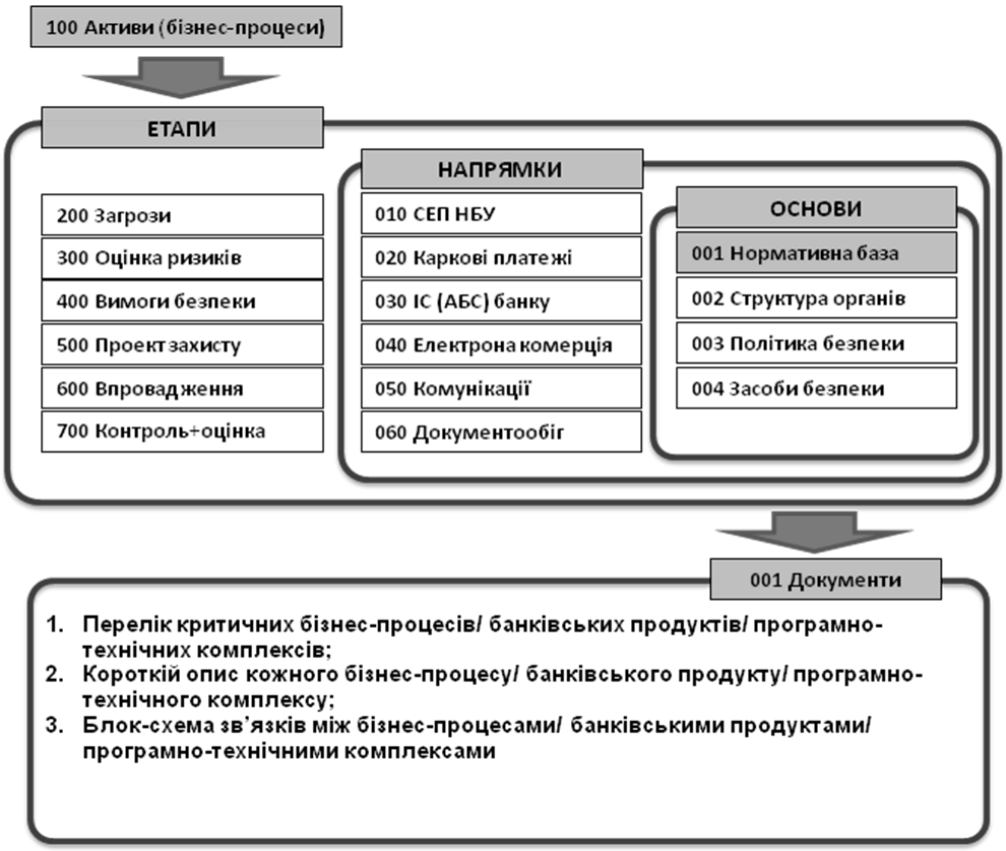


Рис. 4. Процес опису критичних бізнес-процесів та формування відповідних документів

			Відповідальний									
			_Адміністратори		Відділ кадрів		Внутрішній аудит		Підрозділ інформ безпеки		Підрозділ інформ технологій	
Напрямок	Об'єкт	Активи	Заходів		Заходів		Заходів		Заходів		Заходів	
⊟ _Банк в цілому	⊟ Об'єкти ІБ банку	_Активи ІС (АБС)							1			
⊟ _Документообіг	⊟ Комунікації та функції	_Активи ІС (АБС)									2	
	⊟ Об'єкти бізнесу банку	Конфіденційна інформ										
	⊟ Об'єкти ІБ банку	_Засоби СУІБ банку							3			
		Всі активи ІБ банку							1			
		Інфраструктура ІС(АБС)										
	⊟ Об'єкти СУІБ банку	_Засоби СУІБ банку									1	
⊟ _Напрямки бізнесу	⊟ Об'єкти бізнесу банку	Всі активи ІБ банку					1					
	⊟ Обладнання ІС (АБС)	Системи доступу ІС									1	
⊟ _Персонал	⊟ Персонал банку	Всі активи ІБ банку			11							
⊟ ІС (АБС) банку	⊟ Комунікації та функції	Системи доступу ІС									1	
	⊟ Обладнання ІС (АБС)	Компоненти ІС(АБС)							1		1	
		Операційні системи							2		1	
		Прикл прогр користувачив							1			
		Прикладні програми							4			
		Середовище проектування							2		1	
		Система управління ключами							1		2	
		Системи доступу ІС									1	
	⊟ Програмне забезпечення	_Активи ІС (АБС)	14									
⊟ Компютерна мережа	⊟ Програмне забезпечення	_Активи ІС (АБС)	1									
⊟ Комунікації	⊟ Комунікації та функції	_Активи ІС (АБС)							6		34	
⊟ СУІБ банку	⊟ Об'єкти ІБ банку	_Засоби СУІБ банку							8			
		Всі активи ІБ банку							2			
	⊟ Об'єкти СУІБ банку	_Засоби СУІБ банку							4		4	
		Всі активи ІБ банку							3			
⊟ Фізичне середовище	⊟ Режимні приміщення банку	_Режим та охорона										
Общие итоги			15		11		1		39		49	

Рис. 5. Приклад розподілу бізнес-процесів та активів банку за відповідальними

Опис організаційної структури банку, яку охоплює СУІБ

Процес опису організаційної структури банку та розподілу обов'язків з дотриманням системного підходу до ІБ зображено на рис. 6.

Опис організаційної структури банку в СУІБ «Матриця» відбувається шляхом заповнення списку наявних співробітників (підрозділів) банку. Слід розташувати елементи списку відповідно до підпорядкування за допомогою кодів 1-го – 3-го рівнів.

Наприклад: «Адміністратори (05 00)» включають «Адміністратора АБС (05 01)», «Адміністратора мережі (05 02)» і т.д. (рис. 7).

Рис. 6. Процес опису організаційної структури банку та розподілу обов'язків

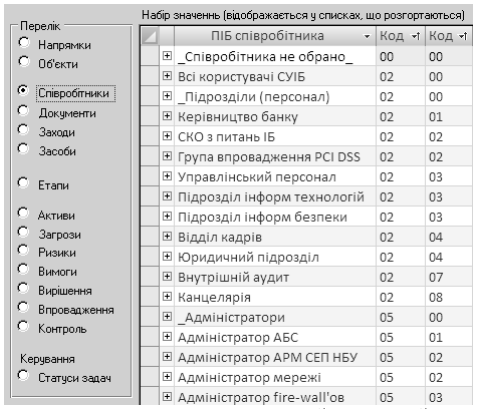


Рис. 7. Приклад опису організаційної структури банку в таблиці «Співробітники»

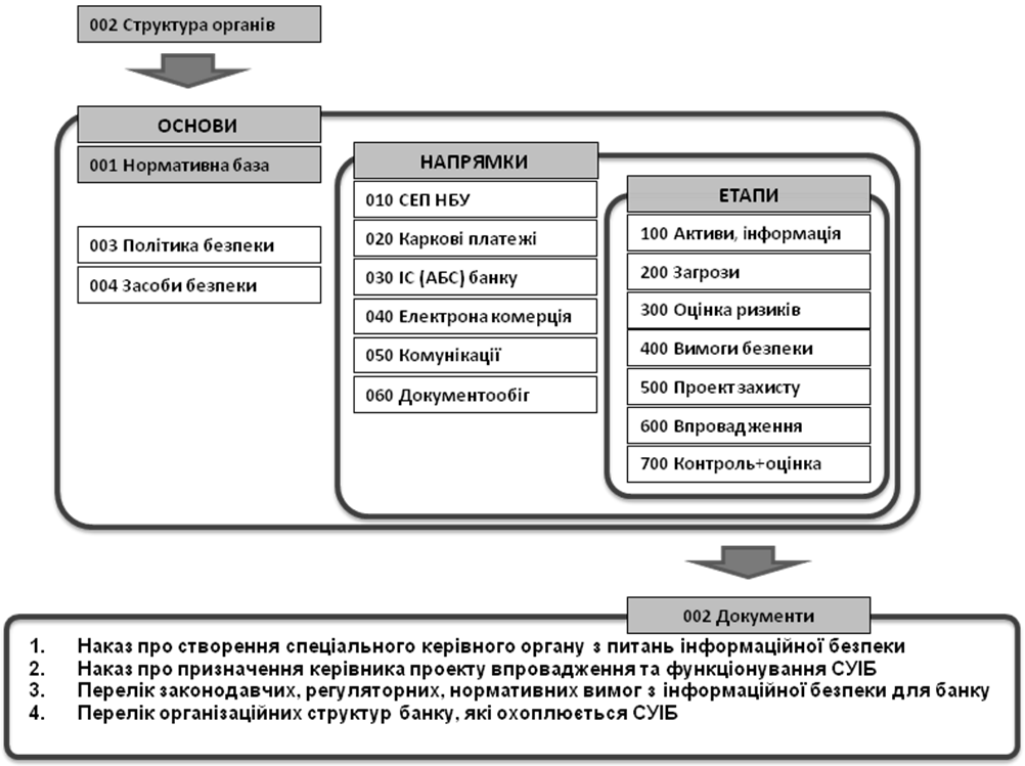


Рис. 8. Процес розподілу обов'язків та створення відповідних документів


Перелік задач

Відповідальний: СКО з питань ІБ

За період з 01.01.100 по 04.02.201

Об'єкти СУІБ банку

4.2 Розроблення та управління СУІБ

4.2.2 Впровадження та функціонування СУІБ

Рис. 9. Приклад звіту, де «СКО з питань ІБ» вказаний як відповідальний за виконання заходів щодо «Впровадження та функціонування СУІБ»

Призначення відповідальних осіб за впровадження СУІБ

Процес розподілу обов'язків та створення відповідних документів з дотриманням системного підходу до ІБ зображено на рис. 8.

Призначення відповідальних за впровадження в СУІБ «Матриця» відбувається наступним чином.

1. Заповнити список співробітників (підрозділів) банку та список вимог, виходячи зі стандартів та, за необхідності, методичних рекомендацій НБУ.

2. Ввести відповідні документи в модуль «Знання» і визначити як мінімум відповідального та вимоги для кожного розділу кожного документа.

3. Призначити відповідальних за задачі впровадження СУІБ за допомогою модуля «Керування».

4. Призначені відповідальні будуть відображатися у сформованих звітах та документах (рис. 9).

5. Статистична таблиця «Вимоги за відповідальними» описуватиме розподіл вимог між підрозділами та працівниками. Є можливість переглянути детальні переліки вимог (рис. 10).

	Документ								
	НБУ СУІБ-1 27001	НБУ СУІБ-2 27002			НБУ Методичні рекомендації		НБУ Методика оцінки ризиків		Общие итоги
Відповідальний	Кількість функцій	Вимоги	Код		Кількість функцій		Кількість функцій		Кількість функцій
_Зовнішні організації		Кількість функцій	1						1
Внутрішній аудит		Кількість функцій	7						7
Всі користувачі СУІБ		Кількість функцій	1						1
Підрозділ інформ безпеки	15	06.1.3 Розподіл відповідальнс	197		2		10		41
		07.1 Відповідальність за актив	122						
		12.1 Вимоги безпеки для ІС	78						
		12.1 Вимоги безпеки для ІС	192						
		12.2.1 Підтвердження вхідних	79						
		12.2.1 Підтвердження вхідних	193						
		12.2.3 Цілісність повідомлень	81						
		12.2.4 Підтвердження вихідни	82						
		12.3.2 Управління ключами	194						
		12.4 Безпека системних файлі	85						
		12.4.1 Контроль операційного	86						
		12.5 Безпека у процесах розр	87						
		[illegible]	[illegible]						
		Кількість функцій	14						
Підрозділ інформ технологій		Кількість функцій	13		2		2		17
Розробники ПЗ		Кількість функцій	1						1
СКО з питань ІБ	1	Кількість функцій			38				39
Управлінський персонал		Кількість функцій	2				2		4
Юридичний підрозділ		Кількість функцій	2						2
Общие итоги	16	Кількість функцій	41		42		14		113

Рис. 10. Приклад таблиці розподілу «Вимог ІБ» за відповідальними з указівками назв документів, що використовуються

Оцінювання ризиків інформаційної безпеки банківської установи

Процес формування змісту нормативних документів щодо оброблення ризиків ІБ банку з дотриманням системного підходу до ІБ зображено на рис. 11.

Оцінювання ризиків в СУІБ «Матриця» засноване на принципах методик [5, 9] та відбувається наступним чином.

1. Заповнити список загроз. В першу чергу включити ті, від яких захищають існуючі системи безпеки, далі додавати ті, що згадуються у використовуваних нормативних документах (статуті підприємства, стандартах, тощо). Також можна використовувати стандартні переліки загроз.

2. Призначити кожній загрозі оцінку частоти її прояву. Рекомендовано умовну шкалу від 1 до 5 балів (рис. 12, а).

3. Заповнити список активів докладним переліком систем, програмно-технічних комплексів та нематеріальних активів банку.

4. Призначити кожному активу оцінку збитку в разі його відмови, пошкодження чи компрометації. Рекомендовано умовну шкалу від 1 до 5 балів (рис. 12, б).

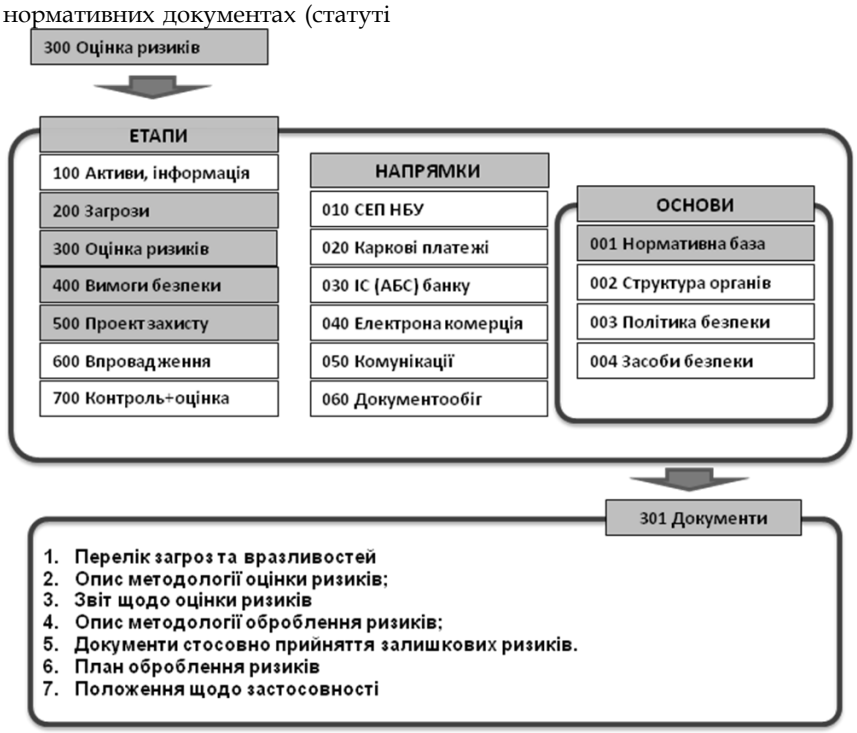
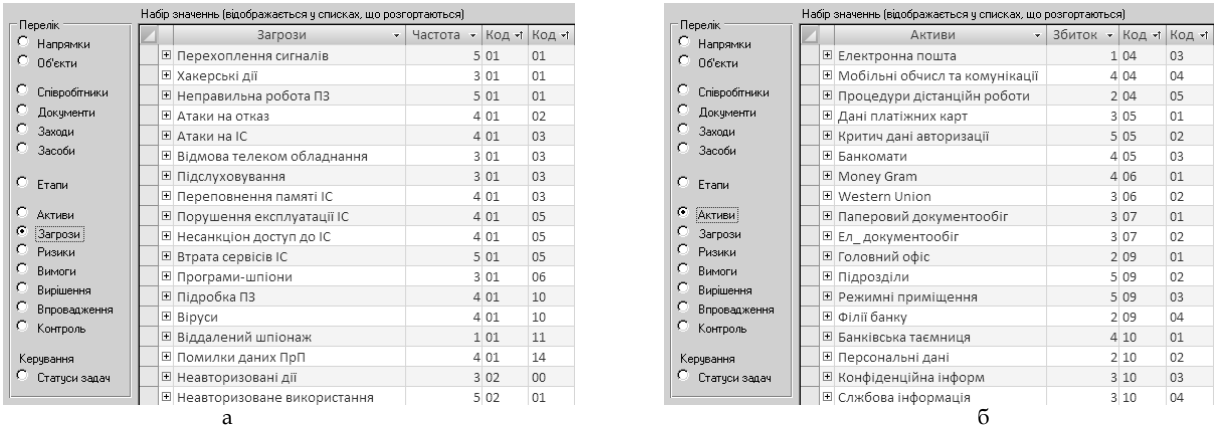


Рис. 11. Процес формування змісту нормативних документів щодо оброблення ризиків ІБ банку



а б

Рис. 12. Приклад переліків загроз (а) та активів (б)

5. Сформувати список ризиків, які розглядаються в банку, з пар «загроза-актив». Оцінки ризиків обчислюються автоматично і будуть відображатися у сформованих звітах та документах.

Примітка: автоматичне формування списку ризиків за перехресним принципом не використовується, оскільки утворюється багато зайвих неможливих ризиків (як, наприклад, пожежа репутації серед клієнтів).

6. Зведена таблиця «Оцінка ризиків» ілюструє розподіл ризиків, що розглядаються в банку, а також надає сумарні оцінки ризиків за загрозами та активами (рис. 13).

7. Зведена діаграма «Оцінка ризиків» дає просте наочне зображення рівня ризиків, а також розподілу їх за активами чи загрозами. Також є можливість фільтрування даних для аналізу окремих сегментів (рис. 14-17).

	Актив																	
	_Активи СЕП НБУ		Всі активи ІБ банку		Ел_ документообіг		Інфраструктура ІС(АБС)		Операційні системи		Прикл прогр користувачив		Системи доступу ІС		Общие итоги	
Загроза	Оцінка ризику		Оцінка ризику		Оцінка ризику		Оцінка ризику		Оцінка ризику		Оцінка ризику		Оцінка ризику		Оцінка ризику	
_Загр Комп'ютерній мережі	25														25	
_Загр СЕП НБУ							15								15	
_Інсайдери	20				12										32	
_Промисловий шпіонаж					15										15	
_Фізичне пошкодження	10														10	
«Чорна пошта»					3										3	
Ввід фальсифікованих даних					12										12	
Віддалений шпіонаж					3										3	
Віруси	20				12										32	
Втрата доступності	20				12										32	
Втрата конфіденційності	15				9								12		36	
Втрата цілісності	25		25		15										65	
Неправильна робота ПЗ									25						25	
Несанкціон доступ до ІС													16		16	
Пожежа	25														25	
Порушення експлуатації ІС							20				20		16		56	
Общие итоги	160		25		93		35		25		20		44		402	

Рис. 13. Приклад оцінки сумарних ризиків по елементах інформаційної інфраструктури банку

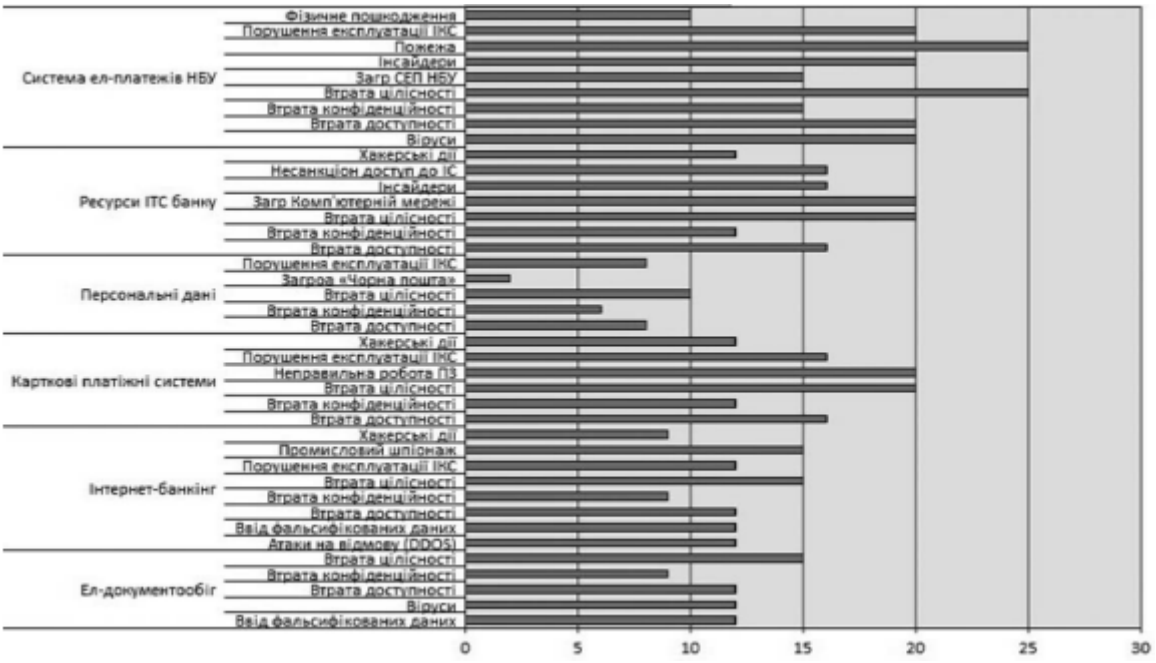


Рис. 14. Графічне представлення оцінки ризиків

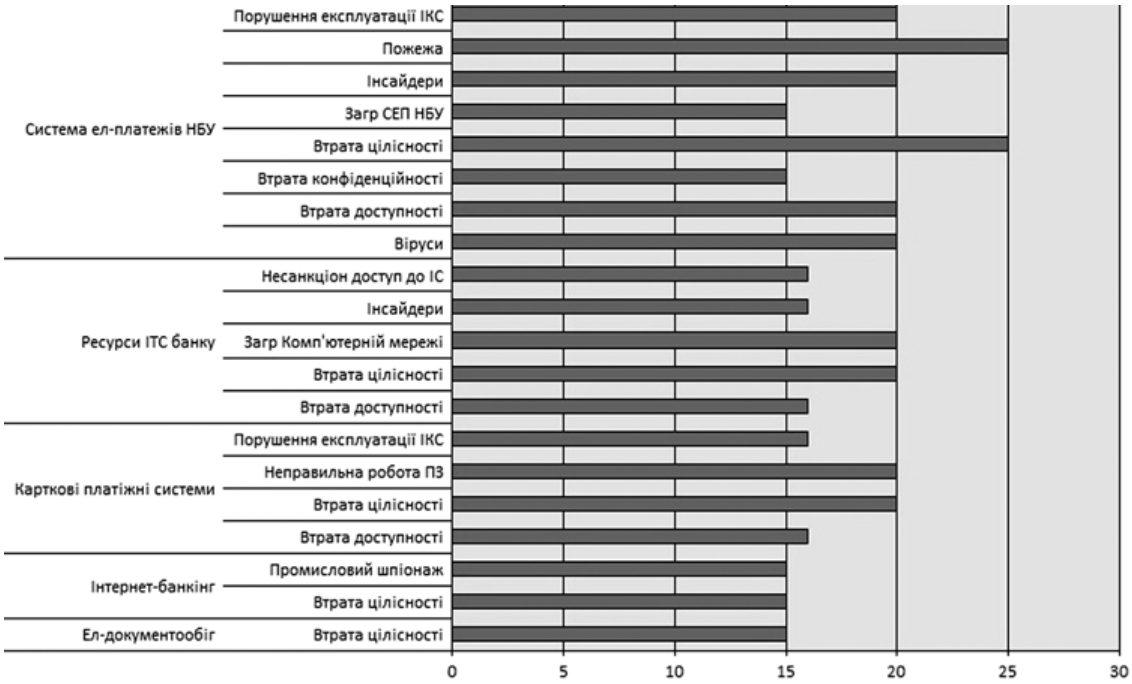


Рис.15. Графічне представлення ризиків, оцінка яких не менше 15

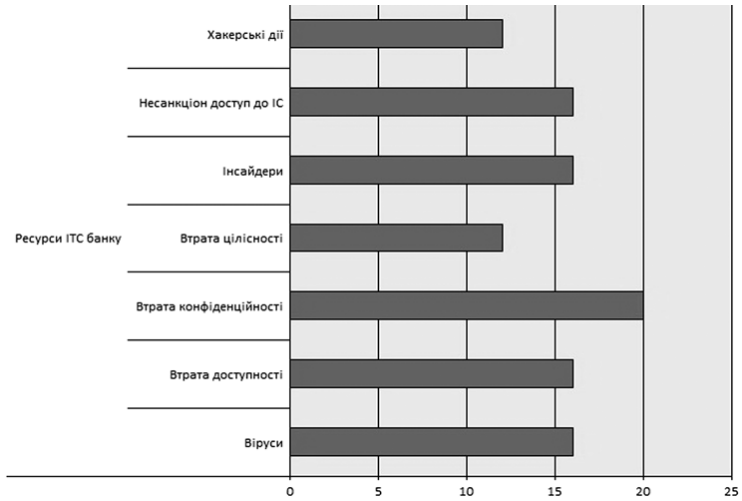


Рис.16. Графічне представлення оцінки ризиків тільки для інформаційно-комунікаційної системи банку

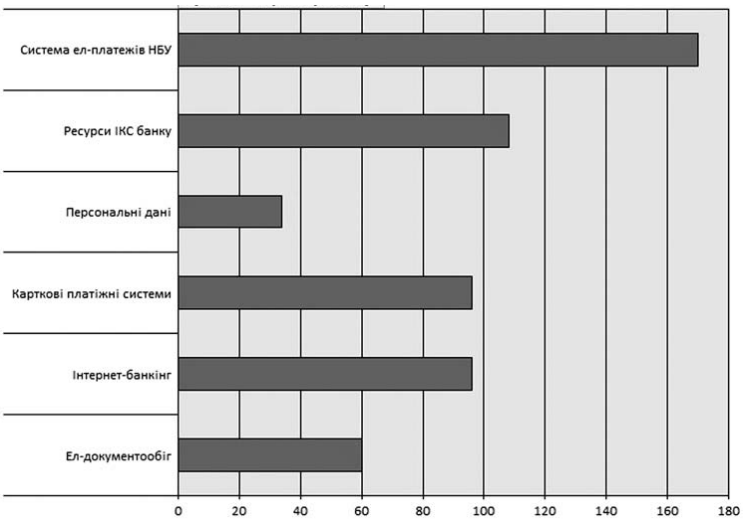


Рис.17. Графічне представлення оцінки активів по сумі ризиків загроз, що їх стосуються

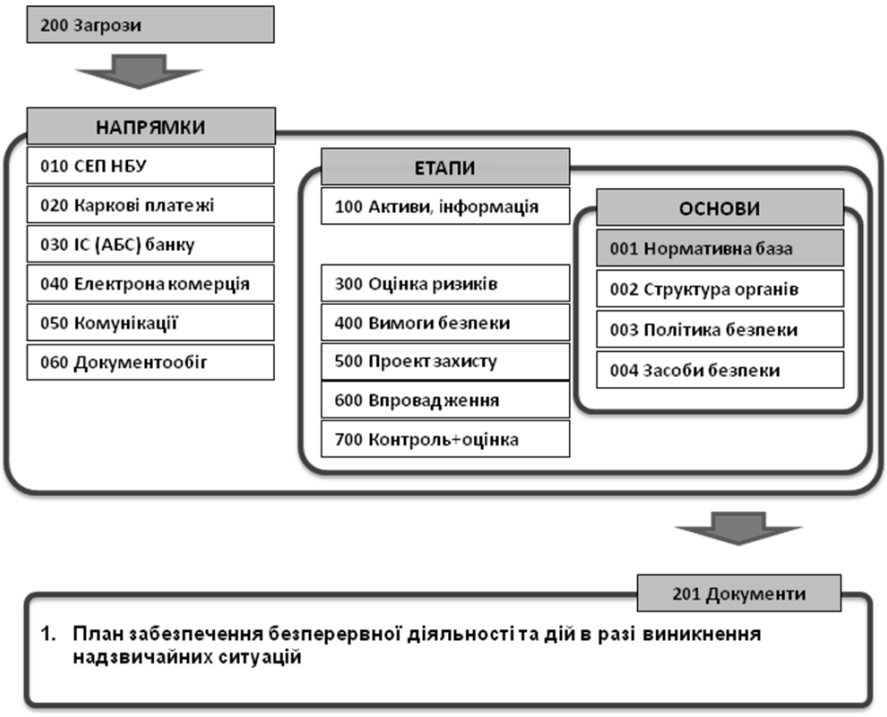


Рис. 18. Процес розробки змісту документа «План забезпечення безперервної діяльності…» відповідно до аналізу загроз ІБ

Плани відновлення у разі надзвичайних обставин

Процес розробки змісту документа «План забезпечення безперервної діяльності…» відповідно до аналізу загроз ІБ з дотриманням системного підходу до ІБ зображено на рис. 18.

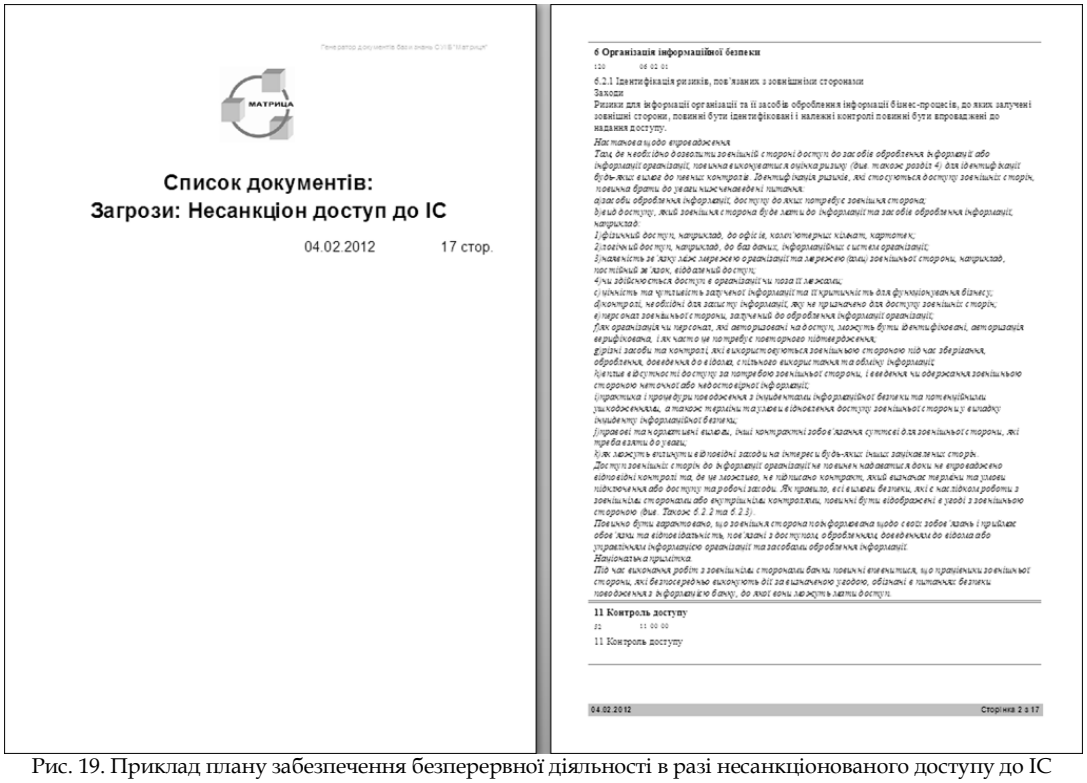
Формування документів на випадок надзвичайних обставин в СУІБ «Матриця» відбувається наступним чином.

1. Доповнити список загроз назвами надзвичайних ситуацій та оцінками частоти їх виникнення.

2. За допомогою модуля «Знання» призначити загрози всім розділам всіх документів.

3. Скомпонувати документ для певної загрози за допомогою форм «Умови відбору» та «Формування документів / звітів».

4. Отриманий документ можна використовувати як план забезпечення безперервної діяльності в разі виникнення конкретної надзвичайної ситуації (рис. 19).


Генератор документів бази знань СУІБ "Матриця"

МАТРИЦЯ

Список документів:
Загрози: Несанкціон доступ до ІС

04.02.2012 17 стор.

6 Організація інформаційної безпеки

120 06 02 01

6.2.1 Ідентифікація ризиків, пов'язаних з зовнішніми сторонами

Заходи

Ризики для інформації організації та її засобів оброблення інформації бізнес-процесів, до яких залучені зовнішні сторони, повинні бути ідентифіковані і належні контролі повинні бути впроваджені до надання доступу.

Настанова щодо впровадження

Також за необхідно дозволити зовнішній стороні доступ до засобів оброблення інформації або інформації організації, повинна виконуватися оцінка ризику (див. також розділ 4) для ідентифікації будь-яких вимог до певних контролів. Ідентифікація ризиків, які стосуються доступу зовнішніх сторін, повинна брати до уваги нижченаведені питання:

а) як саме оброблення інформації, доступу до якої потребує зовнішня сторона;

b) який доступу, який зовнішня сторона буде мати до інформації та засобів оброблення інформації, наприклад:

1) фізичний доступ, наприклад, до офісів, комп'ютерних кімнат, картотек;

2) логічний доступ, наприклад, до баз даних, інформаційних систем організації;

3) взаємність зв'язку між мережею організації та мережею (ами) зовнішньої сторони, наприклад, постійний зв'язок, віддалений доступ;

4) чи здійснюється доступ в організації чи поза її межами;

c) цінність та чутливість залученої інформації та її критичність для функціонування бізнесу;

d) контролі, необхідні для захисту інформації, яку не призначено для доступу зовнішніх сторін;

e) персонал зовнішньої сторони, залучений до оброблення інформації організації;

f) як організація чи персонал, які авторизовані на доступ, можуть бути ідентифіковані, авторизація верифікована, і як часто це потребує повторного підтвердження;

g) різні засоби та контролі, які використовуються зовнішньою стороною під час зберігання, оброблення, доведення до відома, спільного використання та обміну інформації;

h) вплив відсутності доступу за потребою зовнішньої сторони, і введення чи одержання зовнішньою стороною неточної або недостовірної інформації;

i) практика і процедури поводження з інцидентами інформаційної безпеки та потенційними ушкодженнями, а також терміни та умови відновлення доступу зовнішньої сторони у випадку інциденту інформаційної безпеки;

j) правові та нормативні вимоги, інші контрактні зобов'язання суттєві для зовнішньої сторони, які треба взяти до уваги;

k) як захистять взаємовідні інтереси будь-яких інших зацікавлених сторін.

Доступ зовнішніх сторін до інформації організації не повинен надаватися доки не впроваджено відповідні контролі та, де це застосовно, не підписано контракт, який визначає терміни та умови підключення або доступу та робочі засоби. Як правило, всі вимоги безпеки, які є наслідком роботи з зовнішніми сторонами або внутрішніх контролів, повинні бути відображені в угоді з зовнішньою стороною (див. також 6.2.2 та 6.2.3).

Повинно бути гарантовано, що зовнішня сторона поінформована щодо своїх зобов'язань і прийняє обов'язки та відповідальність, пов'язані з доступом, оброблянням, доведенням до відома або управлінням інформацією організації та засобами оброблення інформації.

Національна пам'ятка

Під час виконання робіт з зовнішніми сторонами банку повинні вживатися, що працівники зовнішньої сторони, які безпосередньо виконують дії за вказаною угодою, обізнані в питаннях безпеки поводження з інформацією банку, до якої вони мають доступ.

11 Контроль доступу

12 11 00 00

11 Контроль доступу

04.02.2012 Сторінка 2 з 17

Рис. 19. Приклад плану забезпечення безперервної діяльності в разі несанкціонованого доступу до ІС

Висновки

Надані методичні та практичні рекомендації щодо виконання набору вимог стандартів ГСТУ СУІБ за допомогою СУІБ «Матриця».

Конкретні завдання управління ІБ вирішені з урахуванням особливостей банківських бізнес-процесів та за принципом системного підходу.

СУІБ «Матриця» можна застосовувати як системне рішення для управління ІБ банку шляхом організації взаємодії керівництва банку, підрозділів комп'ютерних (інформаційних) технологій, служби інформаційної безпеки, фахівців внутрішнього аудиту та інших.

Список літератури

[1] Домарев В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – К.: ООО «ТИД «ДС», 2004. – 992 с.

[2] Домарєв В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k) [Текст] / В.В. Домарєв, Д.В. Домарєв. – Донецьк: «Велстар», 2012. – 146 с.

[3] Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) [Текст]: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К.: Національний банк України, 2010. – 49 с. – Код УКНД 35.040.

[4] Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Текст]: ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К.: Національний банк України, 2010. – 163 с. – Код УКНД 35.040.

[5] Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Текст]: лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К.: Національний банк України, 2011.

[6] Domarev D.V. Information security management system "Matrix" based on system approach [Текст] / D.V. Domarev // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2011. – Вип. 2(34). – С. 36 – 39.

[7] Information technology. Security techniques. Information security management systems. Overview and vocabulary [Текст]: international standard ISO/IEC 27000:2009(E). – Geneva: ISO/IEC, 2009. – 26 p.

[8] Information Security Management Systems (ISMS) [Текст]: BSI Standard 100-1, Version 2.0. – Bonn: BSI, 2008. – 38 p.

[9] IT-Grundschutz Methodology [Текст]: BSI Standard 100-2, Version 2.0. – Bonn: BSI, 2008. – 93 p.

УДК 004.056:336 (045)

Домарев Д.В., Домарев В.В. методика управления информационной безопасностью в банковских учреждениях с помощью СУИБ «Матрица»

Аннотация. *Обоснована актуальность вопросов управления информационной безопасностью. Теоретической основой предлагаемой методики является системный подход к информационной безопасности. Для практической реализации предлагаемой методики применена система управления информационной безопасностью «Матрица». Приведены процедуры формирования нормативной базы об информации с ограниченным доступом, описания критических бизнес-процессов и программно-технических комплексов, обеспечивающих их функционирование, описания организационной структуры банка, которую охватывает СУИБ, назначения ответственных за внедрение СУИБ, оценивания рисков информационной безопасности банковского учреждения, создания плана возобновления в случае чрезвычайных обстоятельств. Сделаны выводы о применимости предлагаемой методики в управлении информационной безопасностью банковских учреждений.*

Ключевые слова: *управление информационной безопасностью, СУИБ «Матрица», системный подход к ИБ, система управления информационной безопасностью, формирование нормативных документов, ОСТУ СУИБ, ISO 27000, оценка рисков ИБ.*

Domarev D.V., Domarev V.V. Method of information security management in banking institutions using ISMS "Matrix"

Abstract: *Actuality of information security management is proved. Theoretical basis of the proposed method is the system approach to information security. For the practical realization of the offered method, the information security management system "Matrix" is applied. The following procedures are described: forming of normative base about classified information, description of critical business-processes and hardware/software infrastructures supporting them, description of the bank's organizational structure covered by an ISMS, assignment of staff responsible for the implementation of the ISMS, estimation of information security risks of a banking institution, creation of the emergency recovery plan. Conclusion is made about the applicability of ther proposed method to the information security management in banking institutions.*

Key words: *information security management, ISMS "Matrix", system approach to information security, information security management system, production of normative documents, ISMS branch standard of Ukraine, ISO 27000, information security risk estimation.*

Отримано *12 лютого 2013 року*, затверджено редколегією *14 березня 2013 року*

УМОВИ ІСНУВАННЯ СІДЛОВОЇ ТОЧКИ В БАГАТОРУБІЖНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Євген Левченко[1], Руслана Прус[1], Дмитро Рабчун[2]

[1] Національний авіаційний університет, Україна
[2] Державний університет інформаційно-комунікаційних технологій, Україна

ЛЕВЧЕНКО Євген Григорович, к.ф.-м.н., доцент

Рік та місце народження: 1937 рік, Черкаська область, Україна.
Освіта: Київський державний університет ім. Т.Г. Шевченка, 1959 рік.
Посада: доцент кафедри засобів захисту інформації з 2002 року.
Наукові інтереси: інформаційна безпека.
Публікації: 100 наукових публікацій, серед яких монографія, навчальні посібники, наукові статті та патенти на винаходи.