МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання лабораторних робіт
з навчальної дисципліни
«Менеджмент інформаційної безпеки»

для студентів денної та заочної форми навчання за спеціальністю
125 «Кібербезпека»

ЗАТВЕРДЖЕНО
кафедрою кібербезпеки та
програмного забезпечення,
протокол від 19 січня 2022 року № 10

КРОПИВНИЦЬКИЙ
2022

Методичні рекомендації до виконання лабораторних робіт з навчальної дисципліни “Менеджмент інформаційної безпеки” [для студ. денної та заочної форми навч. за спеціальністю 125 “Кібербезпека”] / Уклад. І. А. Лисенко, В. В. Босько, Л. В. Константинова — Кропивницький: ЦНТУ, 2022.– 33 с.

Укладачі: Лисенко І. А., Босько В. В., Константинова Л. В.

Рецензенти: Смірнов О. А., д.т.н., проф., завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету;
Якименко Н. М., к.фіз.-мат.н., доцент. кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Методичні рекомендації висвітлюють організаційні та практичні аспекти виконання лабораторних робіт з навчальної дисципліни “Менеджмент інформційної безпеки” для студентів денної та заочної форм навчання за спеціальністю 125 “Кібербезпека”, а також пропонують рекомендації щодо ходу виконання робіт, підготовки та представлення отриманих результатів.

ЗМІСТ

Вступ

Для полегшення виконання, оформлення та захисту лабораторної роботи (ЛР) студентам денної та заочної форми навчання необхідно ознайомитись з представленими методичними рекомендаціями.

В методичних рекомендаціях висвітлено організаційні та практичні аспекти виконання ЛР з навчальної дисципліни «Менеджмент інформційної безпеки» для студентів, які навчаються за спеціальністю 125 «Кібербезпека», а також поради щодо ходу виконання робіт, підготовки та вимоги для представлення отриманих результатів.

В рекомендаціях розглядаються: поняття інформаційної безпеки, об’єкти інформаційної безпеки, джерела загроз соціальному і ресурсному об’єктам інформаційної безпеки, інформаційні війни.

Також представлено: класифікація джерел небезпеки ресурсних об’єктів; класифікація інформації за видами доступу; державна таємниця; службова таємниця; комерційна таємниця.

Об’єктно-структурні складові системи інформаційної безпеки.

Базові поняття інформаційної безпеки [1]

	Визначення 1
Безпека	це відсутність загрози або можливість надійно захиститися від неї. Небезпечним слід вважати такий інформаційний вплив, який має дестабілізуючі наслідки, утискає інтереси особистості, суспільства, держави.

	Визначення 2
Інформаційна безпека людини, суспільства, Держави	такий стан їхньої інформаційної озброєності (духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб’єктів.

Визначення 3

“Інформаційна війна”	масоване просування вигідної інформації і замовчування невигідної, цілеспрямована інтерпретація поточних подій.

Таблиця 1

Об’єкти інформаційної безпеки [1]

	Зміст	Джерела загроз	Параметри інформаційної безпеки
об’єкт	*Людина, суспільство, держава*	Частина інформаційного середовища суспільства, яка через низку причин неадекватно відображає світ, який оточує людину	- забезпечення свободи слова та доступу громадян до інформації; - збереження системи цінностей, духовного та фізичного здоров’я особи, суспільства; - запобігання маніпулюванню громадською думкою з боку державної влади, фінансових та політичних кіл
об’єкт	*Інформаційні ресурси, інформаційна інфраструктура*	Комп’ютерна злочинність, фізичне руйнування інформаційної інфраструктури, в т.ч. в результаті дій природних факторів	- захищеність інформаційних мереж, систем управління транспортом, енергетичної та банківської сфер, державного управління, військових формуваньта ін.; - захист великих масивів конфіденційної інформації про особу, що на- них та недержавних Структурах

Таблиця 2

КЛАСИФІКАЦІЯ ДЖЕРЕЛ НЕБЕЗПЕК РЕСУРСНИХ ОБ'ЄКТІВ		
Джерела небезпек	Навмисні	умисні заборонені дії людей, спрямовані на доступ до відомостей, що зберігаються в інформаційній системі
	Випадкові	помилки в діяльності персоналу, збої у роботі обладнання та стихійні лиха
За способами реалізації	Активні	відбувається контакт джерела загроз з елементами інформаційної системи шляхом певного впливу
	Пасивні	без порушення цілісності системи та впливу на її елементи
За впливом	— перехоплення інформації — викривлення або руйнування інформації — блокування доступу до інформації — загроза конфіденційності — загроза цілісності — загроза доступності	

Визначення 4

Режим доступу до Інформації	передбачений правовими нормами порядок отримання, використання, розповсюдження і зберігання інформації

Таблиця 3

Класифікація інформації за видами доступу		
Відкрита інформація	Інформація з обмеженим доступом:	
	Таємна	*Конфіденційна*

Визначення 5

Таємна інформація	містить відомості, котрі становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі

Визначення 6

Конфіденційна Інформація	Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного й іншого характеру, одержаною за власні кошти, або такою, що є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до останньої, включаючи належність її до категорії конфіденційної, і встановлюють для неї систему (способи) захисту.

Види таємниць

Визначення 7

Державна таємниця	це вид таємної інформації, яка охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визнані Законом державною таємницею та підлягають охороні з боку держави.

Визначення 8

Службова таємниця	це вид таємної інформації, що містить відомості економічного характеру (про дислокацію підприємств та їх виробничу діяльність, про запаси продовольства, пропускну здатність шляхів сполучення, корисні копалини та їх розробку тощо); відомості науково-технічного характеру (про відкриття, винаходи, наукові і технічні результати тощо); інші відомості (про заходи у сфері громадської безпеки і громадського порядку, охорони здоров'я, про кадрову політику держави тощо

Визначення 9

Комерційна таємниця	відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам. (Закон України „Про підприємства”)

Таблиця 4

Загрози інформаційній безпеці	- антропогенні; - техногенні; - стихійні

Таблиця 5

КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ	
Зовнішній	безпосередня діяльність недобросовісних конкурентів або злочинних елементів. Їх дії можуть бути спрямовані на: – одержання інформації за допомогою підслуховуючих пристроїв; – викрадення або зняття копій з документів та інших носіїв інформації, що містять комерційну таємницю; – одержання інформації у процесі її проходження через комунікаційні мережі; – знищення інформації або пошкодження її носіїв; – підкуп, шантаж співробітників підприємства з метою одержання інформації, яка містить комерційну таємницю; — переманювання провідних спеціалістів на конкуруюче підприємство.
Внутрішній	пов’язаний з непорядністю окремих співробітників підприємства, незадоволених платнею або відносинами з керівництвом. Вони можуть видати комерційну таємницю конкурентам або знищити важливу інформацію. Іншим внутрішнім джерелом може бути балакучість співробітників, які ведуть службові розмови у невідповідних місцях.

Таблиця 6

Об’єкти забезпечення інформаційної безпеки	- споруди, приміщення і території, на яких розташовані автоматизовані інформаційні системи і де можуть проводитись переговори і обмін конфіденційною інформацією; - технічні засоби автоматизованих інформаційних систем – комп’ютерне обладнання, обладнання локальних мереж, кабельна система, телекомунікаційне обладнання; - програмні засоби автоматизованих інформаційних систем; - інформація, яка зберігається і опрацьовується у автоматизованій інформаційній системі; автономні носії інформації (ком пакт-диски, дискети та ін.); співробітники - організації, які працюють з автоматизованою інформаційною системою і є носіями конфіденційної інформації про захист системи.

Поняття «захист інформації» [1]. Методи захисту інформації. Засоби захисту інформації. Стратегія і тактика захисту інформації у комп’ютерних системах. Компоненти національної інфраструктури захисту інформації

Визначення 10

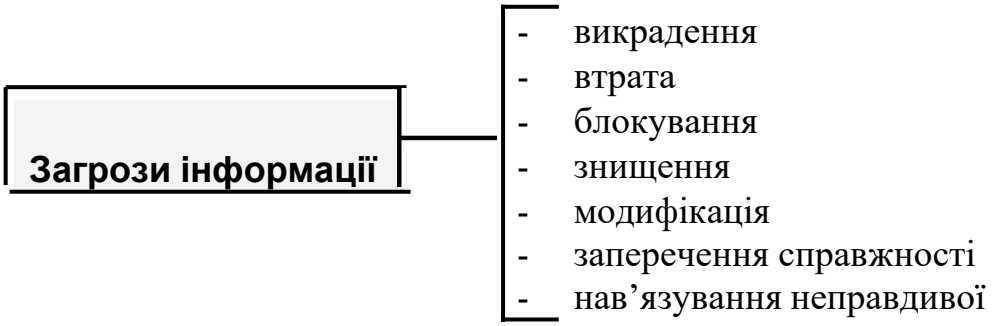
Захист інформації	сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією (*Закон України „Про захист інформації в автоматизованих системах”*).

Таблиця 7


МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ
Організаційні
порядок роботи з конфіденційною інформацією - регламентація доступу у приміщення і безпосередньо до обчислювальної техніки, додержання певних норм і протоколів і відповідальність за їх порушення.
Законодавчі
акти, якими регламентуються правила використання та обробки інформації обмеженого доступу та встановлюються міри відповідальності за їх порушення.
Фізичні
охорона, сигналізація, створення екранованих приміщень для захисту від витікання інформації по каналах випромінювання, перевірка апаратури, що поставляється на відповідність її специфікаціям та відсутність апаратних жучків.
Програмно-апаратні
реалізують технічні (“електронний ключ”) і криптографічні методи захисту.

Таблиця 8

Таблиця 9



Таблиця 10


СТРАТЕГІЯ І ТАКТИКА ЗАХИСТУ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ
На етапі проектування
— визначення переліку і вартості даних, що підлягають захисту;
— аналіз системи як об`єкта захисту та визначення в ній максимально можливої кількості каналів несанкціонованого доступу до інформації і можливих впливів випадкового характеру;
— розробка засобів захисту, що перекривають виявлені канали несанкціонованого доступу і забезпечують заданий рівень безпеки інформації;
— розробка засобів функціонального контролю системи;
— оцінка рівня очікуваної ефективності захисту на відповідність заданим вимогам;
На етапі експлуатації
— контроль і підтримка функціонування системи безпеки інформації у даній комп'ютерній системі;
— своєчасне попередження, виявлення і блокування несанкціонованого доступу;
— реєстрація та облік усіх звертань до інформації, яка підлягає захисту, документування, ведення статистики і прогнозування несанкціонованого доступу.

Таблиця 11

КОМПОНЕНТИ НАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ ЗАХИСТУ ІНФОРМАЦІЇ	
Законодавча компонента	Закон «Про електронний цифровий підпис», «Про електронний документ та електронний документообіг», «Про захист інформації у автоматизованих системах», статті у кримінальному кодексі, закони та підзаконні акти, які регулюють функціонування національної інформаційної інфраструктури
Технічна компонента	Програмні та апаратні засоби криптографічного захисту інформації, розвиток вітчизняної індустрії інформації
Організаційна компонента	Органи, що координують створення і розвиток системи національної інформаційної інфраструктури (Держкомітет, Центр електронних ключів та ін.)
Економічна компонента	Фінансування програм розвитку національної інформаційної інфраструктури, в тому числі розвитку виробництва вітчизняних конкурентоспроможних засобів і систем інформатизації
Методологічна компонента	Концепції і програми розвитку національної інфраструктури захисту інформації, системи ліцензування, сертифікації, системи аудиту безпеки використовуваних технологій, система громадського контролю за розвитком національної інфраструктури захисту інформації

Лабораторна робота № 1

Тема: *Інформаційні ресурси з проблематики захисту інформації у мережі Інтернет*

Мета: Застосовуючи мережуІнтернет навчитись здійснювати аналіз інформаційних ресурсів на доступність та дотримання вимог

Загальні відомості

Подання органами державної влади інформації у мережі Інтернет є одним найбільш дієвих способів взаємодії влади і суспільства [1].

Сайт органу державної влади є відкритим і загальнодоступним інформаційним ресурсом, використання якого здійснюється безоплатно, однак, сайт може містити також інформацію обмеженого доступу.

До сайта органу державної влади висуваються певні вимоги:

— представлення інформації про орган влади, його місцезнаходження, наявність контактної інформації, визначення умов і форм використання матеріалів сайта;

— забезпечення цілодобового контролю за працездатністю сайта;

— з метою запобігання створенню нерівних умов для різних користувачів для доступу до сайта не повинні пред'являтись завищені вимоги до апаратного і програмного забезпечення;

— дотримання принципу поваги до практики інформаційного обміну у мережі Інтернет (відсутність відповідей на звертання громадян і організацій є неприйнятною практикою);

— обмеження на сайті органу державної влади інформації, джерелом якої виступають треті особи (у випадку, якщо така інформація наявна, орган влади повинен визначити межі своєї відповідальності за її повноту і достовірність);

— кожен електронний документ повинен мати власну унікальну адресу, має публікуватись інформація про дату його розміщення, а також забезпечуватись довготривале зберігання оновлюваної інформації;

— розміщення інформації про умови використання сайта.

Пошук *урядових ресурсів* України доцільно починати з урядового порталу України (https://www.kmu.gov.ua/).

Повний список адрес *серверів парламентів* світу представлений на сайті Міжпарламентського союзу (http://archive.ipu.org/english/parlweb.htm).

Пошук *парламентської інформації України* - з сайту Верховної Ради України (https://www.rada.gov.ua/).

Інформаційні ресурси архівів у мережі Інтернет

Архіви зберігають найрізноманітніші види документів з усіх сфер суспільної і особистої діяльності: управлінську документацію, документи особового походження, картографічні документи, науково-технічну документацію, кіно-, фото-, фоно-, відеодокументи, документи церковних конфесій тощо.

Метою функціонування сайтів архівних установ є популяризація архівної справи, розширення доступу громадян і організацій до архівних матеріалів, надання інтерактивних послуг, висвітлення діяльності архівних установ, висвітлення змісту періодичних видань з архівної справи.

Сайти архівів виконують такі функції: надання для широкого кола користувачів науково-довідкового апарату архівів, інформування про діяльність архівних закладів, надання інформації про склад і зміст архівних документів, подання законодавчої, нормативної та методичної бази функціонування архівних установ, висвітлення змісту публікацій (з повними текстами) з архівної справи.

Пошук інформації, яка надається архівами України, можна починати з порталу "Архіви України" (https://archives.gov.ua/ua/).

Бібліотечно-бібліографічні ресурси мережі Інтернет

У мережі Інтернет представлено значну кількість бібліотечно-бібліографічних інформаційних ресурсів як у вигляді бібліотечної реклами, так і з власне бібліографічною інформацією, яка міститься у електронних каталогах. Крім цього, бібліографічна інформація розташовується на серверах наукових і освітніх закладів, які представляють доступ до своєї наукової продукції – періодичним виданням у електронній формі, при чому як на бібліографічному рівні, так і на повнотекстовому.

Бібліографічна інформація може надаватись також серверами видавництв та книготорговельних організацій, спеціальними службами, які забезпечують рефератами або анотаціями журнальних статей та інших друкованих матеріалів та ін.

Сайт найбільшої бібліотеки України – Національної бібліотеки України ім. В.В. Вернадського (http://www.nbuv.gov.ua/), який містить гіперпосилання на провідні бібліотеки світу і України.

Завдання:

1. Ознайомитись з урядовими, парламентськими, архівними та бібліотечними ресурсами мережі Інтернет за наведеними адресами порталів.

2. Проаналізувати представлені ресурси. Порівняти склад і структуру інформаційних ресурсів, до яких надається доступ. Скласти порівняльну таблицю (поставити знаки + та -).

Таблиця 1.1

Тип (назва) ресурсу, web-адреса	Доступ до електронного каталогу або пошук по сайту	Доступ до повних текстів електронних документів	Посилання на інші інформаційні ресурси мережі Інтернет

3. Оформити звіт.

Контрольні запитання:

1. Які вимоги висуваються до сайту органу державної влади?
2. Які види документів зберігають архіви інформаційних ресурсів в Інтернет?
3. Де можна знайти гіперпосилання на провідні бібліотеки світу і України?
4. Що означає поняття безпека?
5. Що означає інформаційна безпека людини, суспільства, держави?

Лабораторна робота № 2

Тема: *Процес управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем*

Мета: За допомогою NIST, CRAMM та OCTAVE, навчитись процессу управління ризиками ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ

Загальні відомості

У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність системи (надалі розглядатимемо бізнес-процес компанії) ефективно функціонувати за умови впливу чинників дестабілізації (ЧД): збої в роботі, руйнування, компрометація тощо та відновлювати таку здатність протягом заданого проміжку часу. Згідно з цим визначенням невід'ємною складовою властивості живучості бізнес-процесу компанії є неперервність його виконання [1]. Міжнародний стандарт ISO 27001, який визначає вимоги до систем менеджменту інформаційної безпеки (СМІБ), тлумачить неперервність функціонування як один із рекомендованих контролів у життєвому циклі СМІБ. Отже, неперервність функціонування є не лише запорукою ефективного розроблення та впровадження СМІБ, але й дієвим способом та невід'ємною складовою процесу забезпечення властивості живучості.

За умов швидкого прогресу сучасного суспільства та високого ступеня інформатизації корпоративні мережі зв'язку (КМЗ) є основним методом збору, оброблення, зберігання та передавання інформації. Водночас, відмітимо важливість такого складового компонента КМЗ, як система захисту інформації (СЗІ), від коректності функціонування якої залежить захищеність інформаційних активів компанії. Тому наголошуємо не просто на властивості живучості організації загалом, а на забезпеченні неперервності функціонування СЗІ в КМЗ як невід'ємній та критично важливій частині ефективного та безпечного функціонування компанії, виконання її основних бізнес-процесів.

Розрізнятимемо такі основні категорії чинників дестабілізації нормальної роботи СЗІ як складової КМЗ в контексті забезпечення їхнього неперервного функціонування [4]:

– Стихійні лиха. Порушення ІБ відбувається внаслідок впливу стихійних лих (наприклад потоп, сильний вітер, блискавка, обвал тощо), що непідконтрольні людині.

– Соціальні заворушення. Порушення ІБ, яке зумовлене нестабільністю суспільства

(наприклад, акти вандалізму, терористичні акти, війни тощо).

– Фізичні пошкодження. Порушення ІБ, яке зумовлене навмисним або випадковим фізичним впливом на СЗІ або її компоненти (наприклад, вогонь, вода, електростатика, вплив навколишнього середовища (забруднення, пил, корозія, замерзання), руйнування, крадіжка, втрата, невміле поводження з обладнанням / носієм інформації).

– Порушення ІБ через відмову базових компонентів СЗІ і послуг, що підтримують функціонування КМЗ (наприклад, відмова мережі

електроживлення, системи кондиціонування повітря, системи водопостачання).

– Порушення ІБ внаслідок порушень, які зумовлені, наприклад, електромагнітним випромінюванням, коливаннями напруги, електронними завадами.

– Технічний збій. Порушення ІБ, спричинене відмовами СЗІ або пов'язаними з нею нетехнічними можливостями. До такого типу ризиків зараховуємо апаратний, програмний збій, перевантаження, порушення ремонтоздатності.

– Технічні атаки. Порушення ІБ, що зумовлене атакуванням КМЗ та використанням її уразливостей в конфігуруванні, протоколах, програмах тощо. Наприклад, мережеве сканування, експлуатація вразливості / бекдору, спроба входу, втручання, відмова в обслуговуванні (DOS / DDoS).

У роботі розглянуто процес управління ризиками ІБ в контексті забезпечення неперервності функціонування СЗІ в КМЗ як невід'ємної складової ефективної та безпечної роботи компанії.

Метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу ЧД. Виділимо чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування КМЗ, зокрема підсистеми СЗІ:

1. Аналіз ризику. Виявлення та оцінка ЧД, які можуть скомпрометувати ІБ важливих інформаційних активів. Дає змогу визначити профілактичні заходи щодо зниження ймовірності виникнення ЧД і визначити контрзаходи з метою успішної нейтралізації цих обмежень ще на етапі проектування.

2. Оцінка ризику. Є процесом визначення рівня ризику. Ризик традиційно обчислюватимемо як функцію важливості активів, ймовірності виникнення загрози і наявності уразливостей, величини завданого збитку.

3. Зниження ризику. Це етап, на якому реалізовуються контролі та заходи щодо запобігання визначеним ризикам, а також впроваджуються засоби відновлення у разі реалізації ризиків, що можуть порушити неперервне функціонування СЗІ.

4. Оцінка уразливостей та контролів. Аналіз основних властивостей КМЗ та виявлення тих, які можна використати з метою реалізації загрози порушення властивості живучості, а також визначення ефективності та адекватності заходів ІБ та виявлення недоліків в її реалізації.

Представимо графічне зображення життєвого циклу процесу управління ризиками ІБ в контексті забезпечення неперервності функціонування (рисунок 2.1).

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30, методика CRAMM та методика OCTAVE [18-19].

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST,

зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems) [1][17]. Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози.

Рисунок 2.1 - Життєвий цикл процесу управління ризиками ІБ

Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий “жорсткий” механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність [8].

Використання такої методики передбачає такі етапи:

- опис характеристик системи;
- ідентифікація загроз;
- ідентифікація уразливостей; аналіз наявних засобів/заходів захисту;
- визначення значення ймовірності;
- аналіз впливу;
- визначення значення ризику;
- вибір засобів/заходів захисту;
- документування отриманих результатів. Алгоритм цієї методики зображено на рис. 2.2.

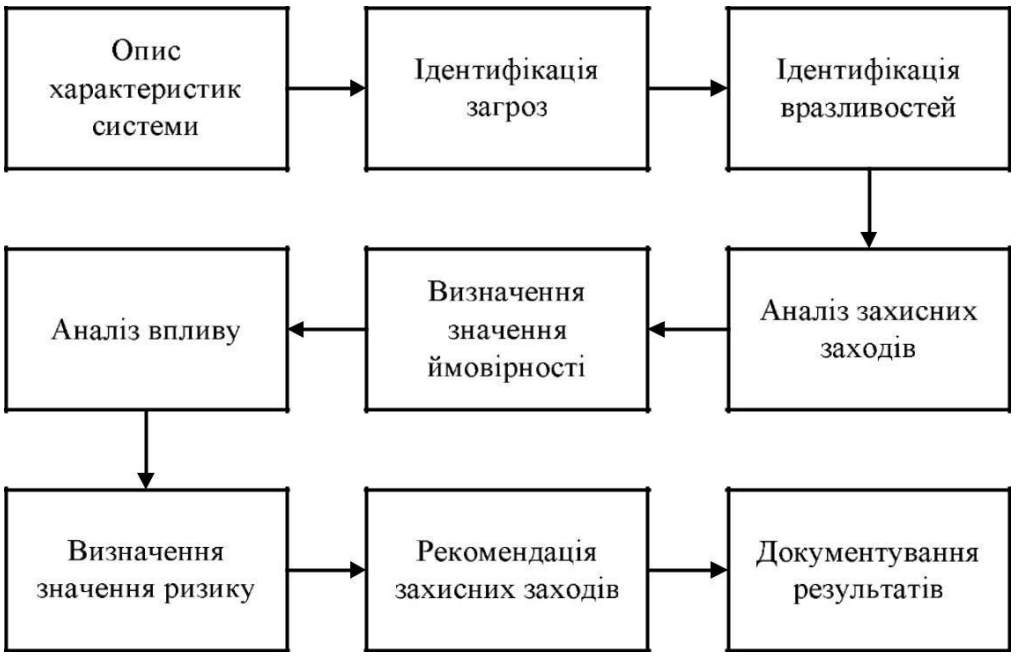


Рисунок 2.2 - Алгоритм методики управління ризиками NIST 800-30

Наступною методикою, яку потрібно проаналізувати є методика CRAMM (CCTA Risk Analysis and Managment Method) [18], яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM [9].

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC ("Помаранчева книга") [9].

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: "Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?" На

другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки і набір звітних документів [7].

Алгоритм методики CRAMM подано на рис. 2.3.

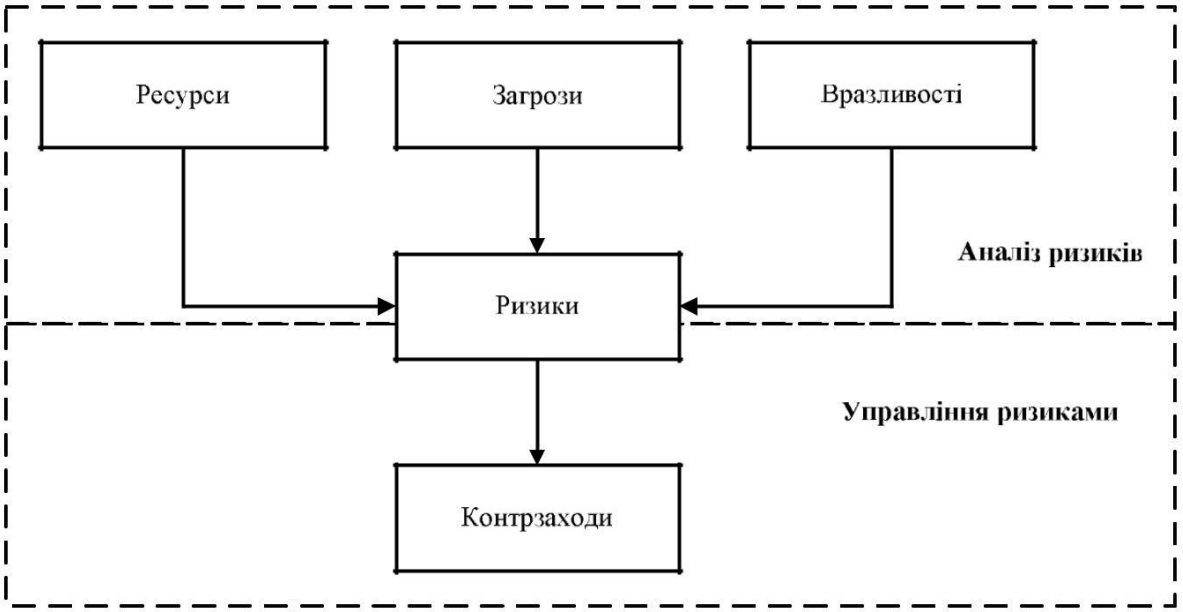


Рисунок 2.3 - Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності [10].

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи [19].

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз уразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних уразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності

завданої шкоди внаслідок реалізації загроз ІБ з використанням уразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

Алгоритм цієї методики зображено на рис. 2.4.

Рисунок 2.4 - Алгоритм методики управління ризиками OCTAVE

Завдання:

Охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки (NIST, CRAMM та OCTAVE) та здійснивши аналіз основних їх властивостей, необхідно визначити основні їх переваги та недоліки і заповнити таблицю 2.1.

Таблиця 2.1 - Переваги та недоліки методик з управління ризиками ІБ

Методика	**Переваги**	**Недоліки**
NIST		
CRAMM		
OCTAVE		

Контрольні запитання:

1. Що означає поняття живучості системи?
2. Який основний метод збору, оброблення, зберігання та передавання інформації?
3. Які чотири основні етапи управління ризиками ІБ, яке здійснюється з метою забезпечення неперервності функціонування КМЗ?
4. Яка методика оцінки ризиків Національного інституту стандартів і технологій США?
5. Що передбачає методикаCRAMM?
6. В чому полягає зміст методики OCTAVE?

Лабораторна робота № 3

Тема: *Моніторинг згадувань об'єктів (інцидентів з інформаційною безпекою) у мережі Інтернет*

Мета: За допомогою моніторингу та інших методологічних засобів навчитись вивчати динаміку ситуацій з інформаційною безпекою

Загальні відомості

Подієвий аналіз є одним із найбільш розповсюджених методологічних засобів вивчення динаміки ситуацій з інформаційною безпекою [1][9]. Методика аналізу ґрунтується на спостереженні за розвитком та інтенсивністю подій (інцидентів з інформаційною безпекою) з метою визначення тенденцій.

Монітоіринг - безперервне спостерігання за станом оточуючого середовища з метою управління ним шляхом своєчасного інформування про можливості настання несприятливих, критичних або неприпустимих ситуацій у галузі ІБ. Моніторингові дослідження широко застосовуються для вивчення різноманітних об'єктів з метою прогнозу їх розвитку [9][10].

Моніторингові дослідження передбачають одержання статистичних або змістових показників, які характеризують об'єкт спостереження і які можна виміряти. Система спостережень будується на фіксації дискретних кількісних характеристик об'єкта спостереження, накопичуванні цих відомостей і на можливості шляхом інтелектуальної інтерпретації одержаних відомостей зробити висновки про якісний стан об'єкта. Моніторинг ґрунтується на спостереженні типових рис у поведінці об'єктів спостереження і на своєчасній фіксації на їх фоні різних відхилень від норми.

Завдання:

1. Визначити об'єкт (особу або подію), відносно якого буде здійснюватися моніторинг.

2. Визначити джерела інформації (наприклад, журнали або ін.), якібудуть використані як інструмент дослідження.

3. Визначити період (напр. 07.12.21-22.02.22. щотижня), протягом якого буде здійснюватися дослідження.

4. Протягом визначеного періоду здійснювати моніторинг згадувань об'єкта (події), кількісні показники.

5. Побудувати графік.

6. Зробити висновки щодо причин і тенденцій динаміки зафіксованих характеристик об'єкта спостереження (зробити звіт).

Контрольні запитання:

1. Що означає подієвий аналіз?
2. Що включає поняття моніторинг?
3. Які об'єкти інформаційної безпеки?
4. Яких типів бувають загрози інформаційній безпеці?

Лабораторна робота №4

Тема: *Інформаційне забезпечення кадрового менеджменту служб інформаційної безпеки на підприємстві*

Мета: Навчитись виконувати дослідження соціально-професійних уподобань членів колективу відділу захисту інформації (служби інформаційної безпеки)

Загальні відомості

З метою атестації, адаптації персоналу і моніторингу ефективності кадрового менеджменту служби ІБ доцільно застосовувати експертні опитування. Основним інтегральним чинником, який позитивно впливає на професійну діяльність особистості, є привабливість для неї самої виконуваної роботи. Компонентами цього чинника є:

1. Чинники прийнятності (необхідні, але не достатні):
   - політика фірми і адміністрації;
   - умови робочого оточення;
   - заробітна платня;
   - міжособистісні відносини (в т. ч. з керівництвом);
   - ступінь безпосереднього контролю за роботою (рівень регламентації, концепція роботи за принципами досягнення заданих цілей, за принципом виконаних завдань тощо);
2. Мотиваційні чинники (достатні для підвищення продуктивності праці):
   - досягнення визнаного особистого успіху;
   - просування по службі;
   - визнання результатів роботи;
   - високий ступінь відповідальності;
   - можливість творчого зростання.

Завдання: виконати дослідження соціально-професійних уподобань членів колективу відділу захисту інформації (служби інформаційної безпеки) і порівняти їх з результатами таких самих досліджень у США і ЕС.

Хід роботи:

1. Для оцінки відносної значущості чинників привабливості роботи необхідно виконати ранжування чинників (за 10-бальною шкалою: 1 – мінімальна значущість, 10-максимальна) і порівняти з результатами опитування працівників у США і ЕС.

2. Оцінити і порівняти ранги чинників (таблиця 4.1).

Таблиця 4.1

№ п/ П	Чинники, які роблять роботу більш Привабливою	Робить роботу більш привабливою					Стимулює працювати більш інтенсивно				
		Працівник 1	Працівник 2	.....	Працівник N	**Середнє**	Працівник 1	Працівник 2	.....	Працівник N	**Середнє**
1.	Робота без значних напружень і стресів										
2.	Зручне розташування										
3.	На робочому місці немає шуму і будь-яких забруднень оточуючого середовища										
4.	Робота з людьми, які викликають Симпатію										
5.	Хороші відносини з безпосереднім Керівництвом										
6.	Достатня інформація про те, що взагалі відбувається у фірмі										
7.	Гнучкий темп роботи										
8.	Гнучкий робочий час										
9.	Значні додаткові пільги										
10.	Справедливий розподіл обсягів робіт										

3. Виконати аналіз одержаних даних, пояснити результати. Оформити звіт.

Контрольні запитання:

1. Що є основним інтегральним чинником, який позитивно впливає на професійну діяльність особистості?
2. Які компоненти основного інтегрального чинника, який позитивно впливає на професійну діяльність особистості?
3. Які засоби захисту інформації бувають? (Таблиця 8)
4. В чому заключається робота з кадрами в засобах захисту інформації (в таблиці 8)?

Лабораторна робота № 5

Тема: *Організація діяльності відділу управління інформаційними ресурсами та захисту інформації*

Мета: На основі загальносистемних принципів діяльності інформаційно-технологічних підрозділів навчитися формулювати типові завдання діяльності у кожній із підсистем діяльності та визначати перелік умінь, необхідних фахівцю для виконання цих завдань.

Загальні відомості

Інформаційний менеджмент представляє персонал інформаційних підрозділів як один з пріоритетних ресурсів, який реалізує інформаційну стратегію організації.

Управління інформаційним персоналом організації – комплекс управлінських заходів, які забезпечують відповідність кількісних і якісних характеристик персоналу та спрямованості і мотивації його професійної діяльності цілям і завданням організації.

Система управління інформаційними ресурсами організаційно базується на розробці положення про відділ управління інформаційними ресурсами та захисту інформації. Зміст діяльності і призначення відділу визначається, виходячи з таких підсистем загальної системи діяльностей: документно-інформаційні ресурси – управління інформаційною діяльністю – комунікації.

З метою підвищення ефективності діяльності організацій пропонується введення посади ***CIO*** (*Chief Information Officer*) – професійного менеджера, який має системний стратегічний погляд на бізнес, поєднує компетенції менеджера і фахівця з захисту інформації, інформаційних потоків і структур, бере на себе відповідальність за формування інфраструктури для створення єдиної захищеної інформаційної системи підприємства, відповідає за організацію всіх інформаційних потоків всередині організації, за її представлення у зовнішньому середовищі, відповідає за забезпечення інформацією всіх функціональних спеціалістів компанії і керівників; має знання і навички формування і використання інформаційних ресурсів в управлінні підприємствами і бізнес-процесами.

Відповідно до загальної структури організації та завдань, що перед нею постають, спрямованість діяльності відділу управління інформаційними ресурсами може визначатись у таких напрямах: відділ зв'язків з громадськістю, інформаційно-аналітичний відділ, інформаційна служба, яка працює за принципом інформаційно-технологічного підрозділу, що спеціалізується на збиранні, обробці, зберіганні та розповсюдженні документальної, документально-фактографічної і фактографічноїінформації, маркетинговий відділ тощо.

Мета роботи: на основі загальносистемних принципів діяльності інформаційно-технологічних підрозділів, які спеціалізуються на збиранні, обробці, зберіганні і розповсюдженні документальної, документально-фактографічної і фактографічної інформації для цілей інформаційно-аналітичного забезпечення сформулювати типові завдання діяльності у кожній із підсистем діяльності, визначити перелік умінь, необхідних

фахівцю для виконання цих завдань.

Завдання:

1. Визначити перелік типових завдань діяльності, які будуть виконуватись відділом відповідно до об'єкту діяльності: документно-інформаційні ресурси – управління інформаційною діяльністю – комунікації. Типові завдання діяльності описані функціями менеджменту (планування, організація, контроль, захист).

2. Відповідно до кожного з об'єктів діяльності та типових завдань діяльності обрати із списку (або визначити самостійно) відповідні вимогидо персоналу, визначити уміння і навички, які повинні мати працівники, які будуть працювати у відділі управління інформаційними ресурсами.

3. Заповнити таблиці (приклад - табл. 5.1, 5.2, 5.3).

Таблиця 5.1 - Документно-інформаційні ресурси

Типове завдання діяльності	**Уміння**
- планування комплексу інформаційних ресурсів для забезпечення цілей діяльності організації - аналіз інформаційних потреб користувачів	
- організація інформаційного забезпечення діяльності організації і її співробітників; - створення умов для зберігання нормативної, довідкової та архівної інформації; - автоматизована підтримка технологічних процедур роботи з документами;	
- контроль використання інформаційних ресурсів;	
- захист інформаційних ресурсів;	

Таблиця 5.2 - Управління інформаційною діяльністю

Типове завдання діяльності	**Уміння**
-розробка стратегічних напрямів розвитку інформаційної діяльності організації,	
-здійснення ділових контактів підприємства із зовнішнім Середовищем -здійснення окремих робіт з розробки і впровадження інформаційних систем, Веб-сайта організації та ін.;	
-управліннядіяльністюпідрозділів,якіздійснюють інформаційну діяльність, розробка посадових інструкцій Співробітників	
-контроль інформаційної безпеки організації;	

Таблиця 5.3- Комунікації

Типове завдання діяльності	Уміння
-застосування інформаційних технологій для здійснення ефективних комунікацій як всередині організації, так і з зовнішнім середовищем; -планування зовнішніх і внутрішніх комунікацій, підтримка доступу до віддалених інформаційних джерел і фондів;	
-організація комунікацій у глобальному інформаційному середовищі мережі Інтернет; -адаптація інформаційних ресурсів підприємства до розповсюдження їх через глобальні інформаційні мережі	
-комунікації у процесах управлінських рішень; -оцінка ефективності основних комунікативних каналів	

Контрольні запитання:

1. Що представляє собою поняття інформаційний менеджмент?
2. Управління інформаційним персоналом організації це…
3. На чому організаційно базується система управління інформаційними ресурсами?
4. За що відповідає людина на посаді ***CIO*** (*Chief Information Officer*)?

Лабораторна робота № 6

Тема: *Планування заходів аудиту інформаційної безпеки*

Мета: Набути навичок планування заходів аудиту інформаційної безпеки та визначення стану захищенності підприємства

Загальні відомості

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам.

В деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства (сегментів його мережі, окремих серверів, баз даних, Інтернет сайтів і т.п.) і надійності засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень і т.п.). Однак ми надалі виходимо з того, що аудит інформаційної безпеки є комплексним (по можливості, вичерпним) дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

Розрізняють ***два основних види аудиту***: внутрішній (проводиться виключно силами співробітників підприємства) і зовнішній (здійснюваний сторонніми організаціями).

Цілями аудиту можуть бути:

• встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків і визначення напрямків подальшого розвитку системи захисту інформації;

• перевірка керівництвом підприємства і іншими зацікавленими особами досягнення поставлених цілей в сфері інформаційної безпеки, виконання вимог політики безпеки;

• контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;

• сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним та міжнародним стандартам).

(Загальні відомості щодо аудиту системи інформаційної безпеки на підприємстві викладено у лекції №11).

Завдання:

1. Підготовка плану заходів щодо аудиту інформаційної безпеки:а) Вибір однієї з представлених компаній.

б) Формулювання вимог аудиту на підставі одного із стандартів інформаційної безпеки.

в) Розробка плану заходів із зазначенням термінів, підрозділів і видів перевірок для обраної компанії.

2. Розробка підсумкового звіту за результатами аудиту:

а) Підготовка найпростішої методики аналізу результатів аудиту.

б) Підготовка форми аудиторського звіту із зазначенням персоналу,його заповнює, і плану проведення повторних перевірок.

3. Усі результати оформити у звіт.

Опис компаній:

1. Компанія має 5 представництв, всі п'ять в різних країнах (.com, .ua і т.д.). Має 5 представництв в кожному від 50-100 чол. Головна компанія 1000 чол в Україні. Відділ продажів у регіональному представництві, адміністративний відділ і відділ обробки даних. Напрямок діяльності компанії - транснаціональні вантажні перевезення.

2. Компанія має одне представництво в Україні, яке є компанією, купленою роком раніше, що займається розробкою програмного забезпечення. Головна компанія до 500 чол. Представництво - до 300 чол. (Різні бренди). 2 домену - 2 бренду

3. Компанія має головний офіс зі штатом 300 чол. Займається продажем стільникових телефонів. По всій Україні 2000-3000 представництв - магазинів, є упр. Менеджер (локальний відділ Продажів), тарифний відділ і відділ логістики.

4. Компанія - 100 чол. Сфера діяльності аутсорсинг, послуги адміністрування різних систем на базі Майкрософт. Клієнти в більшості країн світу. Компанія забезпечує повну підтримку інфраструктури клієнта.

5. Компанія складається з 3-х філій на території України. ГО у Києві. Чисельність ГО 100 чол., у філіях 20 чол. Займається виробництвом і розробкою засобів аутентифікації. Виробництво в філіях, ГО виконує тількиадміністративні дії.

6. Компанія - холдинг з центральним офісом у м. Києві. Займається створенням та розробкою інтернет-сайтів та в неї входить ще 4 компанії, щознаходяться в 4 країнах світу. У кожній компанії до 50 осіб.

Контрольні запитання:

1. Що являє собою аудит стану інформаційної безпеки на підприємстві?
2. Які є два основних види аудиту?
3. Що може бути цілями аудиту стану інформаційної безпеки на підприємстві?
4. Яким вимогам повинна відповідати організація, що здійснює зовнішній аудит?

Лабораторна робота № 7

Тема: *Аналіз ринку аудиторських послуг в Україні*

Мета: Вивчити послуги ринку аудиторських послуг, познайомитися з роботою компаній постачальниками послуг в сфері інформаційної безпеки

Загальні відомості

Основними послугами, які можуть бути передані на аутсорсинг (як окремо, так і в комплексі), є:

• послуги з проведення комплексних аудитів стану інформаційної безпеки на підприємстві;

• послуги з проведення аудитів (інструментальних перевірок) стійкості і надійності окремих інформаційних підсистем (мереж, програмних і апаратних платформ і т, п,) і засобів захисту інформації, що використовуються підприємством;

• послуги з сертифікації інформаційних систем, вироблених програмних і апаратних засобів захисту інформації;

• консультаційні послуги, пов'язані з формуванням стратегії підприємства в сфері інформаційної безпеки і розробкою політики безпеки;

• послуги з проектування системи захисту інформації;

• консультаційні послуги з вибору та адаптації окремих технологій захисту інформації (криптографії, біометричної ідентифікації і т.п.) відповідно до певних умов ведення бізнесу;

• послуги з впровадження системи захисту інформації, а також впровадження окремих технічних (програмних і апаратних) засобів та реалізації організаційних заходів;

• послуги з поточного адміністрування, підтримки та супроводу інформаційних систем і систем захисту інформації;

• послуги з реагування на інциденти, пов'язані з порушеннями інформаційної безпеки;

• послуги з навчання керівників підприємства, фахівців служби інформаційної безпеки та IT-служби, а також користувачів інформаційної системи підприємства.

Також ми розглянемо ще два види послуг, пов'язаних із забезпеченням інформаційної безпеки; послуги зі страхування інформаційних ризиків і послуги з підтримки інфраструктури публічних ключів (Public Key Infrastructure, PKI).

Необхідність вдаватися до послуг спеціалізованих фірм, пов'язаних з перевіркою захищеності і надійності окремих елементів інформаційної інфраструктури (серверів, мереж, міжмережевих екранів і т.п.), обумовлена, як правило, наявністю у цих фірм спеціалізованих програмних і апаратних засобів, необхідних для проведення таких перевірок (наприклад, спеціалізованих сканерів вразливостей), а також наявність спеціальних знань та навичок і різнобічного досвіду, накопиченого в процесі практичної роботи при проведенні подібних перевірок на різних підприємствах. Придбання подібного досвіду в рамках одного підприємства, нехай навіть і дуже великого, практично неможливо.

Одним з найбільш ефективних прийомів при проведенні такого роду перевірок є пробне (тестове) подолання захисту, коли перевіряльник імітує певний напад з метою здійснити порушення (зруйнувати базу даних, викрасти конфіденційну інформацію і т.п.). Основними завданнями перевірок такого роду є;

• оцінка ефективності використовуваних технічних (програмних і апаратних) засобів захисту інформації;

• оцінка ефективності роботи фахівців, відповідальних за реагування на інциденти;

• контроль дотримання співробітниками підприємства вимог політики безпеки.

(Загальні відомості щодо аудиту системи інформаційної безпеки на підприємстві викладено у лекції №12).

Завдання:

1. Знайти і вибрати існуючу аудиторську компанію в області IT (будь-якої сфери аудиту).

2. Провести аналіз використовуваних програмно-технічних засобів, нормативних актів, ГОСТів і т.п. при проведенні аудиту цією організацією.

3. Зробити порівняльний аналіз з конкуруючими організаціями.

4. Аналізи, порівняльні таблиці і весь матеріал оформити в документ Microsoft Word.

5. Зробити підсумкову презентацію (12-15 слайдів), що описує, чому потрібно звернутися саме в цю аудиторську компанію.

6. Усі результати оформити у звіт.

Контрольні запитання:

1. Які основні фактори, які зумовили появу у підприємств потреб в послугах сторонніх фірм?

2. Які є недоліки підходу передачі окремих завдань забезпечення безпеки на аутсорсинг?

3. Які основні послуги, які можуть бути передані на аутсорсинг?

4. Яким вимогам повинна відповідати організація, що здійснює аудит?

5. Основні функції програмних засобів, що забезпечують підтримку організаційної роботи в сфері інформаційної безпеки

Список рекомендованих інформаційних джерел

1. Лисенко І.А. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни “Менеджмент інформаційної безпеки” [для студ. денної та заочної форми навч. за напрямом підготовки 6.170103 “Управління інформаційною безпекою”, спеціальністю 125 “Кібербезпека”] / Уклад. І. А. Лисенко — Кропивницький: ЦНТУ, 2017.— 30 с.

2. Андрианов В.В. Обеспечение информационной безопасности бизнеса / В.А. Андрианов, С.Л. Зефиров, В.Б. Голованов – М.: ЦИПС и Р: Альпина Паблишерз, 2011. – 373 с.

3. Аугустинайтис А., Абарюс П. Информационный менеджмент: наука и преподавание [Електрон. ресурс]. - Спосіб доступу: URL: http://www.nbuv.gov.ua/

4. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.

5. Гринберг А.С. Информационный менеджмент: Учебное пособие для вузов/ А.С. Гринберг, И.А. Король. - М.: ЮНИТИ- ДАНА, 2003. - 415 с.

6. Информация: поиск, анализ, защита/ Авт.-сост. И.Н. Кузнецов. - Мн.: Амалфея, 2004. - 314 с.

7. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. –- К.: Кондор, 2004. –- 384 с.

8. Лодон Дж. Управление информационными системами: Учебник/ Дж. Лодон, К. Лодон. - 7-е изд. - СПб.: Питер, 2005. - 912 с.

9. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособ. для вузов. – М: Горячая линия - Телеком, 2004. – 280 с.

10. Матвієнко О. Інформаційний менеджмент: аналіз предметної галузі//Вісник Книжкової палати. - 2004. - № 8. - С. 13-17.

11. Матвієнко О.В. Концепція менеджменту інформаційних систем в контексті загальних проблем інформатизації суспільства//Вісник Книжкової палати. - 2002. - №10. - С. 17-20.

12. Мельник Л.Г. Экономика информации и информационные системы предприятия: Учебное пособие/ Л.Г. Мельник, С.Н. Ильяшенко, В.А. Касьяненко. - Суми: Университетская книга, 2004. - 400 с.
13. Методика информационной безопасности / Сост. Ю.С. Уфимцев, В.П. Буянов, Е.А. Ерофеев и др. – М.: Экзамен, 2004. – 544 с.
14. Правове регулювання інформаційної діяльності в Україні. - Київ: Інком Інтер, 2001. - 688 с.
15. Ярочкин В.И. Информационная безопасность: Учебник. - М.: Академический Проект: Фонд "Мир", 2003. - 640 с.
16. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p. 4
17. Swanson M. NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems / M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes. – 2010. – 149 p.
18.CCTA Risk Analysis and Management Method [Електронний ресурс] – Режим доступу: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysis-management-tool-cramm/103133 (дата звернення: 21.01.2022)
19. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 1999. – p.
20. Матвієнко О.В., Цивін М.Н. Основи менеджменту інформаційних систем: навчальний посібник. Київ: Центр навчальної літератури, 2005. 176с.
21. Дорофеев А. В. Марков А. С. Менеджмент информационной безопасности: основные концепции Вопросы кибербезопасности. 2014 №1 (2). С. 67-73