МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ

МЕТОДИЧНІ ВКАЗІВКИ

ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ
З ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА»
(частина 1)

для магістрантів спеціальності
121 Інженерія програмного забезпечення
усіх форм навчання

Луцьк - 2022

УДК 004-049.5

М 54

Методичні вказівки до виконання лабораторних робіт з дисципліни «Інформаційна безпека» (частина 1) для магістрантів спеціальності 121 Інженерія програмного забезпечення всіх форм навчання [Електронний ресурс] / уклад. Н. О. Маслова, Т. В. Алтухова. – Луцьк: ДонНТУ, 2022. – 60 с.

Наведено завдання до виконання лабораторних робіт з дисципліни «Інформаційна безпека», надано порядок виконання робіт, перелік літературних джерел, вимоги до оформлення звітів, базові приклади. Завдання орієнтовані на закріплення теоретичного матеріалу та придбання навичок з контролю стану захищеності інформаційної системи й виконання базових завдань дисципліни.

Укладачі: Н.О. Маслова, доцент кафедри ПМІ, к.т.н., доцент
Т.В. Алтухова, доцент кафедри ПМІ, к.т.н.

Рецензент: Шамаєв В. В., доц. кафедри комп’ютерної інженерії, к. т. н., доц.

Відповідальний за випуск: О. А. Дмитрієва, д.т.н., проф., зав. каф. прикладної математики і інформатики

Затверджено на засіданні навчально-методичного відділу ДонНТУ,
протокол № 10 від 31.05. 2022 р.

Ухвалено на засіданні кафедри прикладної математики та інформатики,
протокол № 5 від 23.05.2022 р.

ЗМІСТ

ВСТУП 4
ЛАБОРАТОРНА РОБОТА 1. ЗАКОНОДАВЧА БАЗА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 5
Порядок виконання лабораторної роботи 1 5
Вимоги до оформлення звіту 9
ЛАБОРАТОРНА РОБОТА 2. ІДЕНТИФІКАЦІЯ АКТИВІВ 10
Порядок виконання лабораторної роботи 2 10
Вимоги до оформлення звіту 13
ЛАБОРАТОРНА РОБОТА 3. АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 14
Порядок виконання лабораторної роботи 3 14
Вимоги до оформлення звіту 16
ЛАБОРАТОРНА РОБОТА 4. РОЗРАХУНОК РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 17
Порядок виконання лабораторної роботи 4 17
Вимоги до оформлення звіту 25
ЛАБОРАТОРНА РОБОТА 5. ФОРМУВАННЯ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 26
Порядок виконання лабораторної роботи 5 26
Вимоги до оформлення звіту 30
ЛАБОРАТОРНА РОБОТА 6. КОНТРОЛЬ ВИКОНАННЯ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 31
Порядок виконання лабораторної роботи 6 31
Вимоги до оформлення звіту 32
СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ 34
ДОДАТОК А. Анкета «Стан захисту інформації» 39
ДОДАТОК Б. Цілі заходів безпеки та заходи безпеки 43
ДОДАТОК В. Вимоги до оформлення звітів 58
ДОДАТОК Г. Приклад оформлення титульного листа 60

ВСТУП

Метою навчальної дисципліни «Інформаційна безпека» є надання знань та вмінь, які утворять теоретичний і практичний фундамент, необхідний для управління інформаційною безпекою та побудови систем захисту інформації.

Методичні вказівки спрямовані на формування у студентів базових компетенцій та навичок в галузі захисту інформації та інформаційної безпеки. Сприяють розвитку здатностей до абстрактного мислення, проведення теоретичних та прикладних досліджень на сучасному рівні. Методичні матеріали спрямовані на вдосконалення підходів у проведенні захисту інформаційних ресурсів та здатності до професійного спілкування з представниками відповідних професійних груп у галузі інформаційної безпеки.

Програмними результатами вивчення дисципліни має стати застосування сучасних професійних стандартів й нормативно-правових документів, які регулюють відношення в інформаційній безпеці. Студенти повинні опанувати й системно застосовувати методи аналізу та моделювання елементів систем захисту. Обґрунтовувати вибір програмно-апаратних інструментальних та обчислювальних засобів для ефективного виконання конкретних задач інформаційної безпеки. Проводити аналітичні дослідження параметрів функціонування інформаційно-комунікаційних систем та систем безпеки. Вміти приймати організаційно-управлінські рішення в умовах невизначеності й ймовірності реалізації ризиків інформаційної безпеки.

Виконання завдань, які ввійшли в методичні вказівки дозволяють отримати навички розв’язання сучасних задач захисту інформації, вміння оформлювати прийняті рішення у вигляді комплекту політик безпеки організації чи підприємства; проводити внутрішній аудит згідно розробленої політики.

Вивчення дисципліни надає знання з основоположних принципів побудови та функціонування системи інформаційної безпеки, функціональних можливостей та управління модулями створених систем.

ЛАБОРАТОРНА РОБОТА 1. ЗАКОНОДАВЧА БАЗА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета роботи: Отримати навички з застосування правової бази інформаційної безпеки, ознайомитись з Законом України «Про інформацію».

Порядок виконання лабораторної роботи 1:

1. Ознайомитись з теоретичним та законодавчим матеріалом за темою та виконати наступні Завдання.

Завдання 1.

Знайти відповіді на сформульовані у варіанті (табл. 1.1) питання (Закон України «Про інформацію» від 2 жовтня 1992року N 2658-XII).

Завдання 2.

Вибрати варіант задачі (табл. 1.2) та розв’язати аналітично.

Відповіді на поставлені в задачі питання повинні бути повними, обґрунтованими, з посиланнями на розділи законодавчого акту, що регулюють вказану ситуацію. Визначити наслідки та правову оцінку ситуації, що описана в задачі.

2. Сформувати короткий звіт-презентацію з відповідями на Завдання.

Презентація має включати 1-5 слайдів з ПІБ доповідача, вхідними питаннями та повними, обґрунтованими відповідями на них (обов’язково вказати статтю та пункт закону, що надає відповідь на питання, пояснити висновки).

Приклад вирішення Завдання 2

Задача:

На закритому хімічному підприємстві, яке розташоване в межах міста і яке знаходиться поблизу від державного кордону, в результаті аварії стався викид шкідливих речовин в атмосферу. Міська адміністрація вжила необхідних заходів

з евакуації громадян із заражених територій і запобігла витоку небажаної інформації про аварію. При цьому вона заборонила керівництву підприємства передавати вітчизняним та зарубіжним ЗМІ інформацію про масштаби аварії та відомості, що стосуються життя населених пунктів, які входять в зону досяжності поширення шкідливих речовин. Водночас адміністрація, приймаючи таке рішення, посилалася па закритість виробництва хімічного підприємства. Чи правомірні дії міської адміністрації з точки зору норм інформаційного права?

Хід вирішення задачі. Відповідно ст.8 Закону України «Про державну таємницю», інформація про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян – є відкритою. Також відповідно ст.21 Закону України «Про інформацію», до інформації з обмеженим доступом не можуть бути віднесені відомості про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей.

Висновок. Дії міської адміністрації є неправомірними.

Таблиця 1.1 - Питання до виконання Завдання 1

Варіант	**Питання**	**Стаття, пункт**
1	1. Назвіть основних суб'єктів та об'єкт інформаційних відносин, що визначено Законом	
	2. Наведіть класифікацію інформації за змістом, вкажіть основні види	
	3. Охарактеризуйте поняття та правовий режим інформації довідниково-енциклопедичного характеру	
2	1. Вкажіть основні напрями державної інформаційної політики	
	2. Назвіть основні види інформаційної діяльності, визначені Законом, перелічить їх	
	3. Розкрийте поняття «екологічна» інформація» й чи може вона бути віднесена до інформації з обмеженим доступом?	
3	1. Надайте визначення терміну «Статистична інформація» та вкажіть, чим визначається правовий режим державної статистичної інформації	
	2. Чи може суб'єкт інформаційних відносин вимагати усунення порушень його права на інформацію й який пункт Закону це регламентує ?	
	3. Якими законодавчими актами визначається правовий режим інформації про товар (работу, послугу)?	

Продовження таблиці 1.1 –

Варіант	Питання	Стаття, пункт
4	1. Надайте визначення терміну «соціологічна інформація» та як визначається правовий режим інформації цього виду у Законі ?	
	2. Надайте визначення поняттю «Персональні дані», розкрийте його	
	3. Чи може бути право на інформацію обмежене й якщо так, то за яких умов	
5	1. Надайте визначення поняттю «Науково-технічна інформація», вкажіть, який режим доступу до інформації цього виду рекомендує Закон	
	2. Розкрийте поняття «відкрита інформація» та надайте класифікацію інформації за порядком доступу	
	3. Право одержання, використання, поширення, зберігання та захисту інформації є одним з принципів _____	
6	1. Надайте визначення поняттю «конфіденційна інформація» та вкажіть порядок її поширення відповідно законодавству	
	2. Що передбачає поняття «право на інформацію»? Поясніть його. Вкажіть ситуації, які відносяться до зловживання правом на інформацію	
	3. Сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України називається _____	
7	1. Надайте визначення поняттю «Правова інформація» та вкажіть джерела її надходження, які визначено Законом	
	2. Чи існують підстави звільнення від відповідальності у разі розголошення інформації з обмеженим доступом, надайте пояснення ситуації згідно Закону.	
	3. Орган державної влади, місцевого самоврядування, або інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства називається_____	
8	1. Надайте законодавчі визначення поняттям «масова інформація» та «засоби масової інформації»	
	2. Назвіть умови, яких треба дотримуватись при реалізації права на інформацію	
	3. Назвіть відповідальність, яку тягне за собою факт порушення законодавства України про інформацію?	
9	1. Згідно Закону «Про інформацію» сформулюйте Основні принципи інформаційних відносин	
	2. Чи існують відомості, які за Законом не можна віднести до інформації з обмеженим доступом? Якщо так, назвіть та охарактеризуйте їх	
	3. Надайте відповідь на питання: «Чи потребує центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику **згоди** фізичних осіб на отримання та обробку їх персональних даних ?»	

Продовження таблиці 1.1 –

Варіант	Питання	Стаття, пункт
10	1. Перелічить загальні терміни, які виділено у Законі та надайте їм роз'яснення	
	2. Вкажіть особливості її поширення й розголошення інформації з обмеженим доступом. Надайте визначення суспільно необхідної інформації	
	3. Сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї формують поняття _____	

Таблиця 1.2 - Завдання 2 «Задачі з інформаційної безпеки»

Варіант	Задача	Стаття, пункт
1	Наприкінці року по телебаченню повідомили, що всі борги по зарплаті працівникам бюджетної сфери погашені, але вчителі області оголосили страйк у зв'язку з невиплатою заробітної плати за останні чотири місяці. …….Журналіст Горитько звернувся до адміністрації області з проханням надати йому документи, що містять докладні відомості про соціальні виплати та використання бюджетних коштів області за минулий рік. Йому в цьому проханні відмовили, посилаючись на те, що запитувана інформація є інформацією обмеженого доступу. *….Чи правильні дії адміністрації області та чи законна вимога журналіста? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Сформулюйте пояснення.*	
2	Підприємство вирішило розширити сферу діяльності й створити підрозділи у сусідній області з заправки картриджів. З метою моніторингу ринку запросило в обласному бюро статистики офіційну інформацію про кількість фірм з обслуговування комп'ютерної техніки та заправки картриджів у регіоні, але отримало відмову *Чи відповідають дії статистичного бюро діючому законодавству? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	
3	Позаштатний кореспондент Гаврилов К.І. на протязі трьох років збирав інформацію щодо застосуванню сучасних технологій захисту в промисловій сфері України й вирішив надрукувати наукову статтю з оглядом технологій з цього напрямку. Але редакція журналу, куди направлено роботу, статтю відхилила з огляду на те, що Гаврилов К.І., не є фахівцем у цьому напрямку та не має права претендувати на публікацію в науковому виданні. *Чи є дії редакції правомірними? Надайте оцінку ситуації. Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	
4	Студент Черкаського політехнічного університету в для написання кваліфікаційної роботи звернувся до бібліотеки навчального закладу з проханням підібрати йому наукові публікації викладачів університету за десятирічний період. Працівники бібліотеки студенту відмовили в проханні, сказавши, що ці публікації для студентів не є відкритими і надаються тільки з дозволу авторів. *Чи правомірними с дії працівників бібліотеки з точки зору інформаційно-правових відносин? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	

Продовження таблиці 1.2 –

Варіант	Задача	Стаття, пункт
5	На хімічному підприємстві сталася масштабна пожежа. Хмара з продуктами горіння та попіл «накрили» поля найближчих фермерських господарств. Міська адміністрація, посилаючись на закритість виробництва хімічного підприємства, запобігла витоку небажаної інформації про пожежу. При цьому вона заборонила керівництву підприємства передавати вітчизняним та зарубіжним ЗМІ інформацію про стан довкілля та ступінь шкідливості продуктів горіння. *Чи правомірні дії міської адміністрації ? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	
6	У центральному архіві міста N змінився головний архіваріус. Першою директивою нового керівника став наказ про утилізацію друкованих видань більш 5ніж п'ятирічної давнини, інформаційних бланків, документів з архівних фондів, що втратили свою актуальність. *Чи законні дії головного архіваріуса? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	
7	Група студентів-геодезистів була направлена на практику у місто Львів для проведення геодезичних польових досліджень. Цікавим дослідникам здався район поблизу аеропорту, але на мапах, що розповсюджуються через книгарні, деякі зони було нанесено не детально. Студенти звернулись до кадастрового центру, але отримали категоричну відмову. *Чи є відмова кадастрового центру у наданні детальних мап означеної місцевості законною? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	
8	Студент Київського університету імені Т. Шевченка в ході написання дипломної роботи звернувся до бібліотеки навчального закладу з запитом – підібрати йому неопубліковані роботи та іншу інформацію, яка стосується діяльності Спеціального інформаційного бюро у роки Великої Вітчизняної війни. В бібліотеці студебнту відмовили в проханні, сказавши, що ці джерела знаходяться в спеціальному сховищі бібліотеки, до яких студенти не мають доступу. *Чи правомірними с дії працівників бібліотеки з точки зору інформаційно-правових відносин? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	
9	Держрадіокомпанія досить багато років працює в галузі телебачення та радіомовлення. У зв'язку з скрутним фінансовим станом, дефіцитом приміщень, та вважаючи на те, що більш 70% фахівців компанії є літні люди, компанія не оновлює обладнання, електронний архів веде вибірково, більшість матеріалів зберігає у паперовому вигляді з терміном зберігання – три роки . *Чи законні дії радіокомпанії? Вкажіть законодавчі акти й статті (розділи, пункти) Законів, що регулюють ситуацію. Надайте пояснення.*	

Вимоги до оформлення звіту

1) Титульний лист
2) Вступ (важливість законотворчості в галузі інформаційної безпеки)
3) Основний розділ, в якому надано дані згідно Завдання до виконання роботи
4) Висновки
5) Перелік застосованої літератури.

Література до Лабораторної роботи 1: [1-3]

ЛАБОРАТОРНА РОБОТА 2. ІДЕНТИФІКАЦІЯ АКТИВІВ

Мета роботи: збір та аналіз даних про стан моделі інформаційної системи, формулювання задачі захисту інформації, ідентифікація активів, визначення класу системи безпеки об'єкту дослідження.

Порядок виконання лабораторної роботи 2:

Згідно варіанту завдання до лабораторної роботи та наявності власних обчислювальних пристроїв виділити гілку інформаційної системи для аналізу рівня безпеки. Зібрати та задокументувати необхідні характеристики, виконуючи пропоновану послідовність дій (пп.1-10).

1. Ознайомитись з варіантом завдання до аналізу гіпотетичної інформаційної системи умовного підприємства (табл. 2.1).
2. Сформулювати задачу аналізу стану захищеності обраного об'єкту. До складу системи, яка аналізується, включити не менш п'яти об'єктів захисту (робочі станції, сервери, програмовані засоби телекомунікаційного зв'язку й т.п). Передбачити наявність в системі комп'ютера керівника (викладача) та/або системного адміністратора й можливість включення до системи й отримання інформації з застосуванням власних пристроїв (персонального ПК, ноутбуку, телефону, планшету й т.п.). Передбачити зв'язок системи з керівниками (викладачами) з застосуванням електронної пошти, сайту, соціальних мереж, хмарних сховищ та обмін відомостями між колегами. Скласти перелік об'єктів та ресурсів системи, оформити у вигляді таблиці (табл. 2.2).
3. Визначити та ідентифікувати інформаційні ресурси й інформаційні потоки, що присутні на ресурсах об'єкту захисту. Відобразити структурну схему об'єкту захисту й описати її функціонування.
4. Обрати СУБД та засіб програмування та розробити загальну структуру бази даних та програму (модуль) створення та заповнення табл. 2.2 й накопичення в ній інформації з метою подальшого застосування.
5. Отримати фактичні технічні характеристики обраних ресурсів,

інформацію щодо системного та прикладного програмного забезпечення, яке встановлено та ресурсах. Сформувати відповідні інформаційні таблиці (табл. 2.3, табл. 2.4). Передбачити графу «Вартість» й заповнити її для кожного ресурсу інформаційної системи.

6. Додати інформацію щодо користувачів ресурсів та їх кваліфікації, сформувати табл. 2.5.

7. Визначити інформацію, що обертається та обробляється в системі та провести класифікацію цієї інформації. Комп'ютер системного адміністратора вважати таким, що має можливість виходу на системи верхнього рівня з обробкою персональних та\або конфіденційних даних. Сформувати табл. 2.6.

8. Навести дані про особливості комп'ютерних мереж (протокол, швидкодія тип з'єднання й т.п.), табл. 2.7.

9. Сформувати та заповнити інформаційні табл. 2.3-2.7.

10. Оформити звіт.

Інформаційні таблиці до Лабораторної роботи 2

Таблиця 2.1 – Перелік умовних підприємств для розробки

Варіант	**Підприємство**
1	Інтернет-кафе « назва »
2	Автобусний парк міста ____назва _____
3	Мережа Інтернет-провайдера «__назва _____»
4	Керівництво аеропортом « назва »
5	Фірма з продажу комп'ютерів «___назва ___»
6	Головне управління банком «__назва банку___»
7	Вищий навчальний заклад « назва »
8	On-line магазин косметики й парфумів (AVON, Oriflame…)
9	Керівництво кінотеатрами міста ____назва _____
10	Центр спостереження за дотриманням прав інтелектуальної власності
11	Мережа магазинів з продажу програмного забезпечення
12	Офіс заводу «Авторемонт»
13	Керівництво морським портом (назва)
14	Фірма по ремонту комп'ютерної техніки «____назва ___»
15	Компанія «Вода Слов'янська»
16	Фірма з обліку поставок квітів з Голандії
17	Магазин музичних товарів
18	Центр керування агрофірмою « назва »
19	Система «Студент – комп'ютерна лабораторія ДВНЗ - викладач»
20	Студент – Система дистанційного навчання (Teams) – викладач»

Таблиця 2.2 − Перелік ресурсів та об’єктів інформаційної системи

ID	Об’єкт	Ресурс	Примітки (Місце розміщення, призначення)
1	Ауд. XXX	Сервер	ПК адміністратора,
2		Робоча станція №__	Учбовий комп’ютер
3			
4		Роутер 1	З функією програмування
5		switch	Мережний комутатор
6	Віддалений (переносний) 1	NoteBook	Власний пристрій, BYOD
7	Віддалений (переносний) 2	Android	Власний пристрій, BYOD

Таблиця 2.3 − Орієнтовні характеристики ПК до лабораторної роботи

ID ПК	Характеристики ресурсів
1	**ПК адміністратора**
	Версія операційної системи,
	Версія БІОС
	Ємність оперативної пам’яті
	Ім'я користувача
	MAC –адреса мережевої карти (або IP-адреса)
	Назва комп'ютера (або гаджету)
	Характеристики процесора (тип, level cache, кол. Ядер й т.п)
	Тип материнської плати
2.	**Робоча станція №__**
	й т.д.

Таблиця 2.4 – Програмне забезпечення ПК

ID ПК	№ п\п	Назва	Розробник	Розмір, Мб	Версія	Рік версії	Ліцензія	Вар-тість, грн	Тип ПЗ
		µTorrent	BitTorrent	643Мб-	3.5.5.45	2005	Adware	585	ІПЗ

Примітка: Тип ПЗ: ІПЗ-інстр.пакети, СПЗ – системне ПЗ, ППЗ – прикладне ПЗ, У - утілити

Таблиця 2.5 – Користувачі та володарі

ID ПК	Назва ресурсу	Користувач	статус	кваліфікація	Рівень прав доступу
		Адміністратор	Постійний	Проф.	1 (найвищий)
		Студент 1	тимчасовий	Студ.	7 (Низький)
		Студент 2	тимчасовий	Студ.	7
		Викладач	персональний	користувач	5

Таблиця 2.6 – Класифікація інформації (Відп.ЗУ «Про інформацію»)

ID	№ п\п	Тип інформації	Тип захисту	доступ	Користувач
			Шифрування	Парольний	
			відкрита		

Таблиця 2.7 – Комп’ютерні мережі

ID	№ п\п	Назва	Мережний профіль	Протокол	Тип безпеки	Діапазон.	Канал	IP - адреса	Швидко-дія

Вимоги до оформлення звіту

1) Титульний лист
2) Вступ (загальна інформація про актуальність організації інформаційної безпеки)
3) Основний розділ, в якому навести:
   - структурну схему об’єкту захисту
   - структуру бази даних;
   - програмне рішення для занесення інформації в Таблицю 2.2;
   - приклад заповнених таблиць 2.2-2.7.
4) Висновки,
5) Перелік застосованої літератури.

Література до Лабораторної роботи 2: [1-16]

ЛАБОРАТОРНА РОБОТА 3. АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета роботи: Ознайомлення з методами виявлення загроз та вразливостей, збір та аналіз даних про стан інформаційної системи.

Порядок виконання лабораторної роботи 3:

Для виділеної та описаної у попередніх роботах гілки інформаційної системи зібрати та задокументувати відомості щодо виявлених загроз та вразливостей з застосуванням однієї з пропонованих методик (згідно варіанту).

1. Провести Інтернет-пошук, знайти та ознайомитись з методиками виявлення загроз та вразливостей й оцінювання ризиків інформаційної безпеки згідно варіанту (табл. 3.1).
2. Написати короткий анонс (3-5 сторінок), де вказати призначення та особливостей функціонування методики, розробника, сферу застосування, характерні риси, етапи виявлення загроз та вразливостей, особливості розрахунку ризиків та наявність відповідного інструментального пакету.
3. Навести скріни екранів, які демонструють роботу інструментального пакету, який реалізує методологію (при його наявності).
4. Згідно рекомендацій авторів методики проаналізувати гілку власної системи, сформувати перелік загроз та вразливостей (не менш 15 – орієнтовно по три на кожний обраний в попередніх лабораторних роботах ресурс), оцінити та вказати ймовірність виникнення загрози та можливий збиток при її реалізації.
5. Розширити розробку, виконану до Лабораторної роботи №2 таблицями з переліком загроз (табл. 3.4), ймовірністю їх реалізації (табл. 3.2) та збитками у випадку виникнення (табл. 3.3). Створити, заповнити й роздрукувати табл. 3.2-3.4.
6. Оформити звіт

Примітка*: Для виявлення ймовірності та частоти проявлення загроз та вразливостей використовувати методи анкетування, аналізу системних журналів, Інтернет- відомості, статистику щодо частоти виникнення обраних видів атак в даному регіоні.*

Інформаційні таблиці до Лабораторної роботи 3

Таблиця 3.1 – Варіанти метод для ознайомлення та опису

Варіант	Методики виявлення загроз й оцінювання ризиків
1	Система Enterprise Risk Assessor
2	Методика оцінювання ризиків OWASP
3	Методика оцінювання ризиків MEHARY
4	Методика оцінювання ризиків Oracle Crystal Ball
5	Методології оцінки ризиків Magerit,
6	Методології оцінки ризиків CORAS
7	Методології оцінки ризиків OCTAVE Allegro
8	Методології оцінки ризиків MSAT (Microsoft Security Assessment Tool)
9	Методології оцінки ризиків Risk Matrix
10	Методика COBRA

Таблиця 3.2 – Ймовірність виникнення загроз (рівень небезпеки), шкала 0-5

Середня частота появи	Ймовірність, шкала 0-5	Рівень небезпеки	Якісна шкала
Даний вид атаки відсутній	0	Неймовірний	0
рідше, ніж раз на рік	1	Малоймовірний	М
близько 1 разу на рік	2	Низький	Н
близько 1 разу на місяць	3	Середній	С
близько 1 разу на тиждень	4	Високий	В
практично щодня	5	Критичний	К

Примітка: *найчатіше пропонується застосування трьохрівневої шкали «низький» - «середній» - «високий» рівень небезпеки (Н – С - В).*

Таблиця 3.3 – Рівень вразливості (збиток)

Рівень вразливості	Опис шкоди
0	Розкриття інформації принесе незначний моральний і/або фінансовий збиток фірмі
1	Збиток від атаки є, але він незначний, основні фінансові операції і положення фірми на ринку не порушені
2	Фінансові операції не ведуться протягом деякого часу, за цей час фірма зазнає збитків, але її положення на ринку змінюється мінімально
3	Значні втрати на ринку і в прибутку. Від фірми йде відчутна частина клієнтів
4	Втрати дуже значні, фірма на період до року втрачає становище на ринку. Для відновлення положення потрібні великі фінансові позики.
5	Фірма припиняє існування

Примітка: *також можливо використання якісної трьохрівневої шкали збитків: «низький» - «середній» - «високий» (Н – С - В).*

Таблиця 3.4 − Перелік виявлених загроз та вразливостей

ID	Назва ресурсу	Вразливість	Загроза	Ймовірність виникнення загрози	Збиток

Вимоги до оформлення звіту

1) Титульний аркуш
2) Введення (про методи виявлення загроз та вразливостей)
3) Основний розділ, в якому:
   - описати спосіб виявлення загроз та вразливостей (з прив'язкою до вимог методики);
   - перелік виявлених загроз та вразливостей, ймовірність їх виникнення (табл. 3.2-3.4)
4) Висновки.
5) Перелік застосованих джерел.

Література до Лабораторної роботи 3: [17-31]

ЛАБОРАТОРНА РОБОТА 4. РОЗРАХУНОК РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Мета роботи*:** Ознайомитися з методами й математичними моделями розрахунку ризиків, розробити власний інструмент розрахунку ризиків інформаційної безпеки

Порядок виконання лабораторної роботи 4:

1. Ознайомтеся з лекційними відомостями щодо розрахунку ризиків, зі стандартом ISO/IES 27005 та матеріалами статей [1 - 5].
2. Згідно варіанту (Таблиця 4.1) оберіть методику розрахунку ризиків й запишіть її математичну модель.
3. **Напишіть програму** розрахунку ризиків інформаційної безпеки з застосуванням обраної методики. Передбачте в програмі завдання параметрів, необхідних для виконання розрахунків (наприклад, перелік загроз, шкалу вразливостей, ймовірність загрози, розмір збитку й т.п.) а також Рівень допустимого ризику.
4. Для спроектованої у попередніх роботах системи виберіть три різноманітних загрози безпеки та для двох ресурсів наведіть приклад розрахунку ризиків інформаційної безпеки з застосуванням розробленого програмного модуля.
5. Оформіть звіт.

Теоретичний матеріал до виконання роботи

Кількісна оцінка величини ризику

Розрахунок ризиків виконується згідно рекомендацій, наведених у Додатку Е Стандарту ДСТУ ISO/IEC 27005 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.

Детальний процес оцінки ризиків інформаційної безпеки передбачає проведення ретельної ідентифікації та визначення цінності активів (табл. 4.1), виявлення загроз та вразливостей інформаційної безпеки (табл. 3.4) , включає оцінку загроз цим активам та оцінку вразливостей (табл. 3.2-3.3).

Результати, зафіксовані в таблицях у подальшому використовуються для оцінки окремих ризиків, оцінки сумарного ризику інформаційної системи, обрання засобів контролю безпеки.

Цінність активів може бути відображена у цінових одиницях або умовною шкалою, як показано у табл. 4.1.

Таблиця 4.1 – Цінність активів

	Умовна шкала	Вартість активу, грн
ЦІННІСТЬ АКТИВУ	0	До 1000
	1	Від 1000 до 5000
	2	Від 5001 до 10000
	3	Від 10001 до 50000
	4	Вище 50000

Наступним етапом є отримання кількісних оцінок значення ризику за однією з методик та створення Таблиці ризиків підприємства (табл. 4.2).

Найпростішим способом розрахунку ризиків є застосування формули:

$$R= L*V, \quad (1)$$

де R (Risk) – значення ризику; L (Likelihood of threat) - Ймовірність загрози; V (Vulnerability level) - Рівень вразливості.

При фактичних розрахунках в якості значення L можливо використання не ймовірності виникнення загрози (ймовірність того, що загроза щодо активу буде реалізована), а, наприклад, очікуваної кількісті спроб реалізації загрози за конкретний період часу (тобто приблизну частоту реалізації загрози даного виду за якийсь період часу).

У випадку, коли намагаються підсилити важливість цінової компоненти, формула розрахунку значень ризику має вигляд:

$$R= L*V *D, \quad (2)$$

де R (Risk) – значення ризику; L (Likelihood of threat) - Ймовірність загрози; V (Vulnerability level) - Рівень вразливості, D – розмір збитку, який, як правило, відображається у грошових одиницях й може співпадати з вартістю активу.

Існують йінші схеми розрахунку ризиків. Наприклад, з застосуванням коефіцієнту ALE (Annual Loss Expectancy).

Побудова Матриці ризиків

Наступним етапом складається таблиця ризиків підприємства (Матриця ризиків). Вона може мати вигляд, як наведено у табл. 4.2.

Зверніть увагу, що у прикладі збиток від реалізації загрози прирівняно до цінності активу.

Таблиця 4.2 – Матриця ризиків

Опис загрози	Збиток (цінність активу)	Ймовірність Виникнення загрози	Міра Ризику = Збиток *Ймовірність)	Позначення
a	b	c	d	e
Спам (переповнення поштової скриньки)	1	4	4	R1
Форматування жорсткого диска з центрального офісу	3	1	3	R2
…	…	…	2	Ri
Ітог :	9	X		

Спочатку за певною шкалою (наприклад, див. табл. 4.1) заноситься значення ЦІННОСТІ АКТИВУ (ЦА) для кожного активу, який знаходиться під конкретною загрозою (колонка (b)).

Далі оцінюється ймовірність виникнення загрози (ЙВЗ), для кожної загрози (колонка (c)) і за отриманими результатами обчислюється міра ризику (колонка (d)) шляхом множення $d = b \times c$.

За результатам обчислень (колонка е) може бути проведено ранжування загроз в порядку відповідної міри ризику й виявлено ризики, що мають бути ліквідовані першочергово.

Аналіз таблиці ризиків підприємства проводиться з застосуванням додаткових параметрів, котри введено й описано нижче:

Y-Рівень допустимого ризику = 7 (задається довільно);

Z- подвійний ризик (Z = Y * 2) ;

X- інтегральний ризик (сума ризиків) ;

Pi - і-я політика безпеки;

Ri - обчислений ризик по і-му рядку.

Якщо Ri> Y - необх. посилення (розробка) Pi

Якщо X> Z - система безпеки в цілому не працює => слід знайти max Ri - змінити Pi => повторити розрахунок ризиків підприємства

На етапі аналізу таблиці ризиків задаються деяким максимально допустимим ризиком, наприклад значенням 7. Спочатку перевіряється кожен рядок таблиці на не перевищення ризику цього значення. Якщо таке перевищення має місце, значить, даний рядок - це одна з першочергових цілей розробки політики безпеки. Потім проводиться порівняння подвоєного значення (в нашому випадку 7*2 = 14) з інтегральним ризиком (осередок «Разом»).

Якщо інтегральний ризик перевищує допустиме значення, значить, в системі безпеки набирається безліч дрібних похибок, які в сумі не дадуть підприємству ефективно працювати. В цьому випадку з рядків вибираються ті, які дають найбільший внесок у значення інтегрального ризику та проводиться спроба їх зменшити або усунути повністю.

Оцінка ризиків з застосуванням матриць з зумовленими значеннями

Для оцінка сумарного ризику інформаційної системи можуть використовуватися матриці з зумовленими (визначеними) значеннями (див. табл. 4.3 – 4.6).

Для кожного активу розглядаються відповідні вразливості і загрози. Знов ж таки застосовуються табл. 3.2 та табл. 3.3.

Для кожної комбінації значень ймовірності виникнення загрози – (ЙВЗ) , коефіцієнту простоти використання вразливості – (ПВВ) та цінності активу – (ЦА) ідентифікується відповідний рівень ризику (міра ризику) на основі шкали від 0 до 8 (відповідно прикладу, наведеному у стандарті).

Приклад 1. Застосування Матриці оцінки Заходів Ризику

Наприклад, якщо цінність активу – (ЦА) визначена на рівні 3, ймовірність реалізації загрози – (ЙВЗ) є високою (а саме - «В»), а простота використання вразливості (рівень вразливості) – (ПВВ) – низькою («Н»), то міра ризику – (МР) буде дорівнювати 5.

Таблиця 4.3 - Матриця оцінки Заходів Ризику (ЗР)

ЙВЗ		Н			С			В		
ПВВ		Н	С	В	Н	С	В	Н	С	В
ЦІННІСТЬ АКТИВУ	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Приклад 2. Застосування матриці визначення ймовірності сценарію інциденту

Другим способом є застосуванням матриці визначення ймовірності сценарію інциденту (ЙСІ) (див. табл. 4.4, де «ДН» (дуже низька), «Н» (низька), «С» (середня), «В» (висока), «ДВ» (дуже висока)), що відповідно означає (дуже малоймовірно), (малоймовірно), (можливо), (ймовірно), (часто).

Таблиця 4.4 - Матриця визначення Ймовірності Сценарію Інциденту

ЙСІ, (ЦА)		ДН (0)	Н (1)	С (2)	В (3)	ДВ (4)
Вплив на бізнес	ДН	0	1	2	3	4
	Н	1	2	3	4	5
	С	2	3	4	5	6
	В	3	4	5	6	7
	ДВ	4	5	6	7	8

Отримане результуюче значення ризику вимірюється за шкалою від 0 до 8 (наприклад, «Н» (0-2); «С» (3-5); «В» (6-8)) і може бути оцінене відповідно до критеріїв прийняття ризику.

Приклад 3. Визначення міри ризику інформаційної системи

Розглянемо приклад, в якому особлива увага приділяється наслідкам інцидентів ІБ та визначенню того, яким системам (активам) слід віддавати перевагу.

Це виконується шляхом оцінки двох значень для кожного активу і загрози, комбінація яких буде визначати бали ($Б_{ij}$), де *i* і *j* – відповідно номер активу і загрози.

Підсумовування всіх балів активів дає можливість визначити МР (міру ризику). Спочатку кожному активу присвоюється параметр ЦА (цінності активу). Для кожного випадку виникнення відповідної загрози визначається показник ймовірності ризику (ПЙР). Він оцінюється виходячи з комбінації ЙВЗ і ПВУ (див. табл. 4.5).

Таблиця 4.5 - Приклад оцінки Показника ймовірності ризику (ПЙР) при відомій ймовірності виникнення загрози та рівні вразливості

ЙВЗ (ймовірність виникнення загрози)	Н			С			В		
ПВВ(простота використання вразливості, рівень вразливості)	Н	С	В	Н	С	В	Н	С	В
ПЙР (показник ймовірності ризику)	0	1	2	1	2	3	2	3	4

На наступному кроці за перетином ліній значень ЦА(цінності активу) і ПЙР в табл. 4.6 присвоюються відповідні бали, після чого вони підраховуються для отримання підсумкових значень з кожного активу (за шкалою (0:8)).

Таблиця 4.6 - Бальник

ПЙР	Цінність активу				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Приклад 4. Розрахунок міри безпеки інформаційної системи

Припустимо, що система С має три активи $А_1$, $А_2$, $А_3$ і існують дві загрози $З_1$, $З_2$ цій системі. Нехай $ЦА_1 = 3$, $ЦА_2 = 2$ та $ЦА_3 = 4$.

Розрахувати Підсумковий бал безпеки системи.

Примітка: *З метою демонстрації ідентичности результатів, які надають табл. 4.3-4.5 в процесі рішення реалізуємо три варіанти отримання результату.*

Розв'язання

1) **Для активу $А_1$**

Розглянем випадок для Актива $А_1$ ($ЦА_1$=3) та загрози $З_1$

1.а) за табл. 4.6.

Якщо для $А_1$ і $З_1$ $ЙВЗ_{11}$ = «Н» та $ПВУ_{11}$ = «С», то значення $ПЙР_{11} = 1$ (див. табл. 4.5).

Бали для $А_1$ і $З_1$ можуть бути визначені з табл. 4.6 на перетині ліній $ЦА_1 = 3$ та $ПЙР_{11} = 1$, тобто $Б_{11} = 4$.

1.б) за табл. 4.3 (Матриця оцінки Заходів Ризику)

ЙВЗ=Н, ПВУ=С, ЦА1=3 $Б_{11}$= 4

1.в) за табл. 4.4

ЦА=3=В, ЙВЗ=Н, ПВУ = С, шкала С: 3-5, МР=$Б_{11}$=4

Таким точно чином, для Актива $А_1$ та загрози $З_2$

Нехай для $А_1$ і $З_2$ $ЙВЗ_{12}$ = «С», а $ПВУ_{12}$ = «В», то

за табл. 4.5 та 4.6 $ПЙР_{12} = 3$, тобто $Б_{12} = 6$.

Табл.4.3: ЙВЗ=С, ПВУ=В, ЦА1=3 отримуємо $Б_{12}$= 6

Табл. 4.4: ЦА=3=В, ЙВЗ = С, ПВУ = В, шкала В: 6-8, маємо Б12=6

Тепер можна обчислити сумарні бали ($БІ_i$) активу $А_1$ щодо всіх загроз

$БІ_1 = Б_{11} + Б_{12} = 10$.

2) Для активу $А_2$

Розглянем випадок для Актива $А_2$ ($ЦА_2$=2) та загрози $З_1$

2.а) Якщо для $А_2$ і $З_1$ $ЙВЗ_{21}$ = «В» та $ПВУ_{21}$ = «С», то значення $ПЙР_{21} = 3$ (див. табл. 4.5).

за табл. 4.6

Бали для $А_2$ і $З_1$ можуть бути визначені з табл. 4.6 на перетині ліній $ЦА_2$ = 2 та $ПЙР_{21}$ = 2, тобто $Б_{21}$ = 5.

2.б) Теж саме за табл. 4.3 (Матриця оцінки Заходів Ризику)

ЙВЗ=В, ПВУ=Н, ЦА1=2, отримуємо $Б_{21}$= 5

Теж саме за табл. 4.4

2.в) Табл.4.4: ЦА=2=С, ЙВЗ = В, ПВУ = С, шкала С: 3-5, маємо МР=$Б_{21}$=5

Таким точно чином, для активу $А_2$ та загрози $З_2$

Нехай для $А_2$ і $З_2$ $ЙВЗ_{12}$ = «С», а $ПВУ_{12}$ = «С», то

за табл. 4.6

$ПЙР_{12}$ = 2, тобто $Б_{22}$ = 4.

Табл.4.3: ЙВЗ=С, ПВУ=С, ЦА1=2, отримуємо $Б_{22}$= 4

Табл.4.4: ЦА=2=С, ЙВЗ = С, ПВУ = С, шкала С: 3-5, маємо $Б_{22}$=4

Тепер можна обчислити сумарні бали ($БІ_i$) активу $А_2$ щодо всіх загроз

$БІ_2 = Б_{21} + Б_{22}$ = 9.

3) Для активу $А_3$

Розглянем випадок для Актива $А_3$ ($ЦА_2$=4) та загрози $З_1$

3.а) Якщо для $А_3$ і $З_1$ $ЙВЗ_{31}$ = «Н» та $ПВУ_{31}$ = «С», то значення $ПЙР_{31}$ = 1 (див. табл. 4.5).

Бали для $А_3$ і $З_1$ можуть бути визначені з табл. 4.6 на перетині ліній $ЦА_3$= 4 та $ПЙР_{231}$ = 1, тобто $Б_{31}$ = 5.

3.б) Теж саме за табл. 4.3 (Матриця оцінки Заходів Ризику)

ЙВЗ=Н, ПВУ=Н, ЦА1=4 , отримуємо $Б_{31}$= 5

Теж саме за Таблицею 4.4

3.в) Табл.4.4: ЦА=4=ДВ, ЙВЗ = Н, ПВУ = С шкала С: 3-5, маємо МР=$Б_{31}$=5

Таким точно чином для активу $А_3$ та загрози $З_2$,

Нехай для $А_3$ і $З_2$ $ЙВЗ_{12}$ = «В», а $ПВУ_{12}$ = «В», то

Табл. 4.6 $ПЙР_{12}$ = 3, тобто $Б_{32}$ = 8.

Табл.4.3: ЙВЗ=В, ПВУ=В, ЦА1=4, отримуємо $Б_{32}$= 8

Табл.4.4: ЦА=4=ДВ, ЙВЗ = В, ПВУ = В, шкала В:6-8, маємо $Б_{32}$=8

Сумарний бал ($БІ_i$) активу $А_3$ щодо всіх загроз

$БІ_3 = Б_{31} + Б_{32} = 13$.

Підсумковіий бал всієї системи: $БІС = БІ_1 + БІ_2 + БІ_3 = 10+9+13=32$

Результат: Підсумковіий бал сумарного ризику всієї системи дорівнює 32 одиниці.

Вимоги до оформлення звіту

1) Титульний лист
2) Вступ (загальна інформація про ризики інформаційної безпеки)
3) Основний розділ, в якому:
   - коротко описати існуючі методики розрахунку ризиків;
   - сформулювати математичну модель обраної методики для написання програми й розрахунку ризиків;
   - описати дані, необхідні для виконання розрахунків й роботи програми;
   - навести код програми з поясненнями;
   - навести результати роботи програмного блоку, допоміжні та результуючу таблиці;
   - сформулювати результати аналізу стану безпеки за значеннями припустимого та подвійного ризику (параметри Y та Z).
4) Висновки
5) Перелік застосованих джерел.

Література до Лабораторної роботи 4: [32-34]

ЛАБОРАТОРНА РОБОТА 5. ФОРМУВАННЯ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета роботи: Закріпити навички поняття «Політики інформаційної безпеки», сформувати документи Політик.

Порядок виконання лабораторної роботи 5:

1. Згідно структури інформаційної системи, для якої проводиться внутрішній аудит, використовуючи наявні знання, зовнішні джерела інформації, елементи побудови системи, яка створена з застосуванням пакетів розрахунку ризиків й пропонованих контрзаходів та лекційний матеріал за курсом, сформувати перелік необхідних Політик та приклади двох документів Політик інформаційної безпеки (один – верхнього, другий – середнього або нижнього рівня).

2. При розробці Політики верхнього рівня рекомендовано передбачити наступні підрозділи документу Політик:

1. Перелік основ для розробки ПІБ (стандартів)
2. Загальні положення
3. Цілі і завдання Політики
4. Основні терміни, скорочення та визначення
5. Порядок організації робочого місця
6. Використання Програмного забезпечення
7. Правила користування електронною поштою
8. Доступ до мережі Інтернет
9. Захист і зберігання даних
10. Віддалений доступ
11. Обов'язки користувача інформаційної системи (ІС)
12. Заборони при роботі в ІС компанії
13. Відповідальність персоналу

Приклад: Політика нижнього рівня

Правила користування електронною поштою

Вступ

Електронна пошта одна з найважливіших засобів комунікації в діловому світі. Повідомлення швидко і зручно передаються по внутрішнім мережам і всьому світу через інтернет. Повідомлення можуть бути перехоплені, записані, прочитані, змінені і перенаправлені кому завгодно, а іноді просто зникнути. Випадкові коментарі можуть бути зрозумілі неправильно і привести до порушення контрактів або судових розглядів.

Основні принципи

- Користувачі електронної пошти повинні уникати діяльність, що порушує інформаційну безпеку.
- Корпоративна електронна пошта повинна використовуватися в рамках посадових обов'язків. Всі повідомлення електронної пошти в інформаційних системах і мережах вважаються власністю підприємства.

Вимоги політики

1. Не використовуйте електронну пошту:

- для відправки конфіденційної / секретної інформації якщо вона не зашифрована криптографічним ПЗ, дозволеним до використання в аудиторії;
- для створення, відправлення, пересилання чи зберігання повідомлень або вкладень, які можуть вважатися незаконними або образливими простими людьми, наприклад, матеріали сексуального характеру, расистські, що дискредитують, образливі, непристойні, принизливі, дискримінаційні, загрозливі, що турбують або інші подібні повідомлення;
- в особистих і благодійних цілях, не пов'язаних з навчальним процесом;
- для розсилки будь-яких підривних, образливих, неетичних, незаконних або інакше неприпустимих матеріалів, включаючи образливі коментарі з приводу раси, статі, кольору, інвалідності, віком, сексуальної орієнтації, порнографії, тероризму, релігійних переконань і вірувань, політичних переконань або про національне походження, гіперпосилань або інших посилань на непристойні або очевидно образливі веб-сайти і подібні матеріали, жарти,

масові розсилки, попереджень про віруси і розіграшів, звернень про допомогу, вірусів або іншого зловмисного програмного забезпечення;

- у будь-яких інших незаконних, неетичних і недозволених цілях.

2. Виявляйте професійну розсудливість при використанні електронної пошти. Дотримуйтеся загальноприйнятих правил етикету при роботі з електронною поштою. Ретельно перевіряйте повідомлення перед відправкою, особливо при спілкуванні з зовнішніми контрагентами.

3. Не розкривайте без необхідності можливу непублічну інформацію в повідомленнях, що йдуть за межі підприємства.

4. Електронні листи автоматично скануються в інформаційних системах на наявність шкідливих програм, спаму і нешифрований службової або особистої інформації. На жаль, процес сканування недостатньо ефективний , тому небажана / сумнівна пошта іноді потрапляє до користувачів. Видаляйте такі повідомлення або повідомляйте про них в службу підтримки.

5. Співробітники не повинні перехоплювати, ігнорувати, змінювати, видаляти, зберігати або публікувати повідомлення крім випадків, санкціонованих керівництвом або з метою адміністрування IT систем.

6. Обмежене використання корпоративної електронної пошти дозволяється під відповідальність керівництва, враховуючи, що це носить випадковий і непостійний характер і не заважає виконанню посадових обов'язків. Всі повідомлення, що відправляються в корпоративних системах і мережах піддаються автоматичному скануванню і можуть бути поміщені в карантин і / або переглянуті уповноваженими співробітниками.

7. Не використовуйте веб-сервіси Mailru, Hotmail, Yahoo або схожі поштові системи третіх сторін (зазвичай звані «вебмайл») в службових цілях. Не надсилайте і не перенаправляйте корпоративну електронну пошту на зовнішні поштові системи / системи третіх сторін. Ви можете користуватися вашою особистою поштовою скринькою з використанням корпоративних систем під відповідальність керівництва з урахуванням, що цей вид використання пошти вкрай обмежений і не вважається особистим використанням.

8. Раціонально підходьте до числа і розміру повідомлень які ви відправляєте і зберігайте. Періодично видаляйте старі повідомлення з вашою поштової скриньки, які більше не потрібні. Відправляйте важливі листи в архів у відповідність з політикою архівування пошти.

Відповідальність

Управління інформаційної безпеки відповідає за дотримання вимог цієї політики. Будучи в тісному зв'язку з користувачами, управління відповідально за освітню діяльність, що має на меті підвищити рівень обізнаності та розуміння відповідальності, визначеної в цій політиці.

Співробітники відповідають за організацію, конфігурацію, використання і обслуговування обладнання для роботи з електронною поштою (включаючи антиспам, антивірус і інші фільтри) у відповідністю з цією політикою.

Служба IT підтримки відповідає за допомогу співробітникам у використанні електронної пошти і служить центральним пунктом збору повідомлень про інциденти з використанням електронної пошти.

Всі співробітники, що мають відношення до цієї політики, несуть відповідальність за дотримання даної та інших корпоративних політик. Справжня політика також відноситься до співробітників третіх організацій, що працюють в тих же умовах незалежно від того чи пов'язані вони з політикою інформаційної безпеки підприємства явно (наприклад, особливими пунктами контрактів) або неявно (наприклад, загальноприйнятими нормами поведінки).

Інформаційна таблиця до Лабораторної роботи 5

Таблиця 5.1 - Приклади назв документів ПІБ

№ з/п	Назви документів
1	Загальна Політика підприємства в галузі інформаційних технологій
2	Комплексна програма забезпечення інформаційної безпеки підприємства
3	Правила роботи користувачів з інформаційною системою «Бухгалтерія»
4	Правила надання доступу та використання ресурсів мережі Інтернет
5	Правила установки і використання програмного забезпечення на підприємстві
6	Положення про використання сторонніх IT-пристроїв (домашніх ПК, планшетів, ноутбуків, смартфонів і т.п.) в діяльності підприємства

Продовження таблиці 5.1 -

№ з/п	Назви документів
7	Правила користування електронною поштою
8	Правила формування, контроль і регламент зміни паролів
9	Правила надання доступу до внутрішньої локальної мережі підприємства
10	Правила користування зовнішніми накопичувачами інформації (флеш-карти, переносні дискові накопичувачі, CD-накопичувачі та ін.) На території підприємства
11	Адміністративні рішення. Комплекс заходів, що застосовуються до порушників ІБ
12	Положення про використання відкритого ПЗ (нові технології)
13	Загальні напрямки організації інформаційної безпеки підприємства
14	Правила організації віддаленого доступу до сервісів ІС підприємства
15	Положення про інформаційну безпеку
17	Правила допуску сторонніх фахівців до ІТ-ресурсів підприємства
16	Правила роботи з електронним Сховищем (базами даних) підприємства (контроль доступу до інформації, розміщеної в БД, права на внесення / зміна / видалення інформації, блокування записів та ін.)
17	Порядок виконання робіт по Системному адміністрування програм і даних
18	Правила роботи з інформаційними ресурсами підприємства.

Вимоги до оформлення звіту

1) Титульний аркуш

2) Введення (про необхідність розробки ПІБ при створенні СУІБ)

3) Основний розділ, в якому:

- обґрунтувати необхідність розробки ПІБ при створенні СУІБ;
- навести перелік Політик, рекомендованих до створення в рамках аналізу Вашої інформаційної системи;
- додати розділ «Рекомендації експертів», який підтверджує зв’язок системи, яка аналізується з пропонованими Політиками;
- прикріпити два документи Політик (один з них – верхнього рівня), які розроблено для аналізованої системи.

4) Сформулювати висновки.

Література до Лабораторної роботи 5: [2-3, 13, 35-40]

ЛАБОРАТОРНА РОБОТА 6. КОНТРОЛЬ ВИКОНАННЯ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета роботи: Проведення контролю інформаційної безпеки з застосуванням стандарту ISO/IEC 27001:2015 Оцінювання рівня інформаційної безпеки підприємства, проведення внутрішнього аудиту

Порядок виконання лабораторної роботи 6:

1. Ознайомитись з Додатком А «Цілі заходів безпеки та заходи безпеки» національного стандарту України ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою. Вимоги».

2. Розробити програмний модуль для створення таблиці «Контрольний список аудиту» згідно Додатку А стандарту України ДСТУ ISO/IEC 27001 та пропонованої на лекційних заняттях структури (Таблиця 6.1).

3. Заповнити таблицю й вказати основні дії, що підтверджують виконання заходів безпеки. З застосуваням програми провести кількісне оцінювання ступеню виконання заходів за кожним розділом (у процентах).

4. Надати мовну оцінку виконання захисних заходів за кожним розділом

5. Отримати загальну оцінку повноти виконання вимог законодавства та рівня захищеності інформаційної системи підприємства.

6. Обговорити результати проведеного аналізу, зробити висновки, надати пропозиції з подальшого розвитку захищеності інформаційної системи підприємства.

Примітка: *Матеріали Додатку А «Цілі заходів безпеки та заходи безпеки» національного стандарту України ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою. Вимоги» додано до методичних матеріалів у вигляді Додатку Б – Матеріали Стандарту для аналізу та опрацювання.*

Інформаційні таблиці до Лабораторної роботи 6

Таблиця 6.1 - Контрольний список аудиту (приклад створення й заповнення)

	Підрозділ	Заходи	Ступінь виконання, %	Примітка
1	2	3	4	5
А.5 Політики безпеки				
А.5.1 Принципи управління інформаційною безпекою				
А.5.1.1	Політики інформаційної безпеки	Заходи безпеки		
		Набір політик щодо інформаційної безпеки повинен бути визначений	50	Всього – 10 ПІБ, виконано 5
		Затверджений керівництвом, виданий і доведений до відома всього найманого персоналу та необхідних зовнішніх сторін	10	Виконано 1 із 1 ПІБ
	Ітого:		***50 %***	***Політики розроблено частково***
А.5.1.2	Перегляд політики інформаційної безпеки	Політики інформаційної безпеки необхідно переглядати в заплановані інтервали часу або за появи істотних змін для забезпечення їх постійної придатності, адекватності і ефективності	50	Виконується за вимогою
	Ітого:		***50 %***	***Переглянуто при аналізі стану ІБ***
	…	…	…	…
	Ітого:		…	…
	Всього:		***50 %***	***Відповідність принципам – частокова***

Примітка: *Заповнення табл. 6.1 виконується у відповідності до розділів Стандарту інформаційної безпеки України ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою. Вимоги»*

Вимоги до оформлення звіту:

1) Титульний аркуш

2) Введення (щодо необхідності менеджменту ІБ)

3) Основний розділ, в якому:

- коротко охарактеризувати стандарт ДСТУ ISO/IEC 27001:2015 взагалі та Додаток А цього стандарту;
- навести таблицю «Контрольний список аудиту» з поясненнями та відповідними розрахунками

- навести та описати код програмного модуля створення таблиці та отримання результату.

4) Сформулювати висновки.

Література до Лабораторної роботи 6: [41-45]

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII із змінами та доповненнями [електронний варіант]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12# Text. – Назва з екрану.

2. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навчальний посібник / В.А. Лужецький, А.Д. Кожухівський, О.П Войтович. – Вінниця: ВНТУ, 2009. – 268 с. Режим доступу: http://ir.lib.vntu.edu.ua//handle/123456789/21843. - Назва з екрану.

3. Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. – Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.

4. Бутенко Л. Л. Структурно-логічні схеми. Таблиці. Опорні конспекти. Есе. Навчальні презентації: рекомендації до складання: метод. посіб. для студ. [Електронний ресурс] / уклад.: Л. Л. Бутенко, О. 2. Г. Ігнатович, В. М. Швирка. – Старобільськ, 2015. – 112 с. Режим доступу: http://dspace.luguniv.edu.ua/jspui/bitstream/123456789/402/1/Strukturno-logichni%20shemu.pdf . – Назва з екрану.

5. Навчальний посібник автоматизація технологічних процесів і систем автоматичного керування (частина 1) [Електронний ресурс]. - Режим доступу: http://kyrator.com.ua/index.php?catid=23&id=696:titulna1&Itemid=130&limitstart=4&option=com_content&view=article . – Назва з екрану.

6. Схеми автоматизації технологічних процесів [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/Схеми_автоматизації_технологічних_процесів. - Назва з екрану.

7. Структура и классификация информационных систем [Електронний ресурс]. - Режим доступу: http://phys.bspu.by/static/lib/inf/posob/stu_m/glaves/glava3/gl_3_2.htm. - Назва з екрану.

8. Как узнать характеристики компьютера, ноутбука [Електронний ресурс]. - Режим доступу: https://ocomp.info/harakteristiki-kompyutera.html. - Назва з екрану.

9. Как узнать полную информацию о компьютере в Windows 10? [Електронний ресурс]. - Режим доступу: https://hetmanrecovery.com/ru/recovery_news/how-do-i-find-out-all-the-information-about-a-computer-in-windows-10.htm. - Назва з екрану.

10. Список нормативних документів щодо інформаційної безпеки в Україні [електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/Список_нормативних_документів_щодо_інформаційної_безпеки_в_Україні. - Назва з екрану.

11. Голев Д. В. Методика оцінки інформаційної захищеності телекомунікацій: Навч. посіб. галузі знань 1601, 1701 «Інформаційна безпека» за спеціальністю 7.17010201, 8.17010201 – Системи технічного захисту інформації, автоматизації її обробки / Д.В. Голев. – Одеса, 2013. – 218 с.

12. Інформаційна безпека: навч. посіб. / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник та ін.; ред. Ю.Я. Бобало, І.В. Горбатий. - Львів: вид-во Львівської політехніки, 2019. - 580с.

13. Лісовська, Ю.П. Інформаційна безпека України: навч. посіб. / Ю.П. Лісовська. - Київ: вид-во Кондор, 2018. - 172 с.

14. Методи безпечної оброрбки інформації у багатопозиційних системах радіолокації: монографія/ І. Пархомей, В. Козловський, С. Гнатюк . – К.: ЦУЛ, 2019. – 230 с.

15. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.

16. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства/ Шаньгин В.Ф. – М-К: ДМК Пресс, 2008. – 544 с.

17. ДСТУ ISO/IEC 27001:2015 Методи захисту системи управління інформаційною безпекою. Вимоги [Електронний ресурс]. - Режим доступу: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf. - Назва з екрану.

18. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія / О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов. - Київ, ЦП «Компринт», 2017. – 435с.

19. Метод COBIT [Електронний ресурс]. - Режим доступу: https://studref.com/377422/informatika/metodika_cobit. - Назва з екрану.

20. Метод CORA [Електронний ресурс]. - Режим доступу: http://coras.sourceforge.net. – Назва з екрану.

21. Метод CRAMM, [Електронний ресурс]. - Режим доступу: www.cramm.com. – Назва з екрану.

22. Методика оценки критических ресурсов, угроз и уязвимостей безопасности информации для малых предприятий (описание и руководство по применению методики: технический отчет). OCTAVE-S / А.В. Потий, Ю.А. Избенко, А.В. Леншин и др. – Х. ХНУРЭ, 2006. – Т. 1. – 144 с.

23. Програмне забезпечення RiskWatch [Електронний ресурс]. - Режим доступу: https://riskwatch.com/. – Назва з екрану.

24. Рахметов Р. Анализ международных документов по управлению рисками информационной безопасности, 2020 [Електронний ресурс]. - Режим доступу: https://habr.com/ru/post/495236/. – Назва з екрану.

25. MAGERIT version 3 (spanish version): Analysis and Risk management information systems [Електронний ресурс]. - Режим доступу: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en. – Назва з екрану.

26. Mehari 2010 Risk analysis and treatment guide (fr) [Електронний ресурс]. - Режим доступу: https://clusif.fr/wp-content/uploads/2015/10/mehari-2010-risk-analysis-and-treatment-guide.pdf. - Назва з екрану.

27. Oracle Crystal Ball [Електронний ресурс]. - Режим доступу: https://www.oracle.com/cis/applications/crystalball/. – Назва з екрану.

28. OWASP risk rating Methodology [Електронний ресурс]. - Режим доступу: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology. Назва з екрану.

29. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments [Електронний ресурс]. - Режим доступу:https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. – Назва з екрану.

30. Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (en). The Software Engineering Institute [Електронний ресурс]. - Режим доступу: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. – Назва з екрану.

31. Ristić, Dejan (2013). "A tool for risk assessment" (PDF). *Safety Engineering*. 3 (3) [Електронний ресурс]. - Режим доступу: https://www.znrfak.ni.ac.rs/SE-Journal/Archive/SE-WEB%20Journal%20-%20Vol3-3/Safety%20Engineering%20Vol03No3.pdf#page=21. – Назва з екрану.

32. Гарасим Ю.Р., Ромака В.А., Рибій М.М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем [Електронний ресурс]//«Львівська політехніка», 2013. Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/23330/1/16-90-99.pdf. - Назва з екрану.

33. Домарєв Д. В., Домарєв В. В., Прокопенко С. Д. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця» [Електронний ресурс]. - Режим доступу: https://www.epos.ua/view.php/about_pubs_archive?subaction=showfull&id=1369342800&archive=&start_from=&ucat=2&. – Назва з екрану.

34. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) [Електронний ресурс]. - Режим доступу: https://www.iso27001security.com/html/27005.html. - Назва з екрану.

35. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с

36. Політика інформаційної безпеки ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» [Електронний ресурс]. - Режим доступу: https://www.pinbank.ua/wp-content/uploads/2017/02/Polityka_IB_2016_2.0_2_KT-1.pdf. - Назва з екрану.

37. Політика інформаційної безпеки акціонерного товариства «БАНК 3/4» [Електронний ресурс]. - Режим доступу: https://bank34.ua/bezpeka-obslugovuvannya/politika-informacijnoi-bezpeki.html. - Назва з ерану.

38. Політика інформаціної безпеки національного університету «Львівська політехніка» [Електронний ресурс]. - Режим доступу: https://lpnu.ua/sites/default/files/2020/pages/2023/svo0601politykainformaciynoyibezpeky.pdf . - Назва з екрану.

39. Політика інформаційної безпеки АТ «Райффайзен Банк Аваль» [Електронний ресурс]. - Режим доступу: https://raiffeisen.ua/storage/files/politika-informatsiynoi-bezpeki.pdf . - Назва з екрану.

40. Політика інформаційної безпеки Акціонерного товариства комерційний банк «ПриватБанк» [Електронний ресурс]. - Режим доступу: https://static.privatbank.ua/files/file.pdf . - Назва з екрану.

41. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

42. Системи менеджменту інформаційної безпеки: навчальний посібник / Ромака В.А., Дудикевич В.Б., Гарасим Ю.Р., та ін.. - Львів: «Львівська політехніка», 2012. - 230 с.

43. Аудит інформаційної безпеки: підручник / Ромака В.А., Лагун А.Е., Гарасим Ю.Р., Рак Т.Є., Самотий В.В., Рибій М.М. – Львів: СПОЛОМ, 2015. – 364 с.

44. Замула О.А. Захист державних секретів. Навчальний посібник для студентів спеціальностей напрямку «Інформаційна безпека»/ О.А. Замула. - Харків. ХНУРЕ, 2003 - 208 с.

45. ДСТУ ISO 19011:2003. Настанови щодо здійснення аудитів систем управління якістю і екологічного управління. – К.: Держспоживстандарт України, 2004. – 31 с.

ДОДАТОК А. Анкета «Стан захисту інформації»

1. Загальні відомості

1.1 Повне найменування організації: _____
_____

1.2 Скорочена назва організації: _____
_____

1.3 Адреса: _____

1.4 Тел. / Факс, e-mail: _____

1.5 П. І. Б. керівника: _____

2. Наявність підвідомчих установ, організацій

2.1 Повне найменування організації: _____
_____

2.2 Скорочена назва організації: _____
_____

2.3 Адреса: _____

2.4 Тел. / Факс, e-mail: _____

2.5 П. І. Б. керівника: _____

3. Наявність об'єктів, що вимагають захисту

3.1 Наявність інформаційних систем, що містять персональні дані.

є _____ (Так/Ні) Кількість _____

3.2 Клас і кількість інформаційних систем персональних даних.

Клас	1	2	3	4
Кількість				

3.3 Наявність ключових систем інформаційної інфраструктури.

є _____ (Так/Ні) Кількість _____

3.4 Наявність інформаційних систем конфіденційної інформації.

є _____ (Так/Ні) Кількість _____

3.5 Наявність інформаційних систем загального користування, підключених до інформаційно-телекомунікаційних мереж, доступ до яких не обмежений певним колом осіб.

_____ (Так/Ні) Кількість _____

3.6 Наявність інформаційних систем, що здійснюють міжвідомчу взаємодію.

_____ (Так/Ні) Кількість _____

4. Наявність структурних підрозділів із захисту інформації та фахівців відповідальних за безпеку інформації

4.1 Наявність структурних підрозділів із захисту інформації.

_____ (Так/Ні) Кількість _____

4.2 Наявність штатних фахівців із захисту інформації.

_____ (Так/Ні) Кількість _____

4.3 Наявність позаштатних спеціалістів із захисту інформації.

_____ (Так/Ні) Кількість _____

4.4 Кількість штатних / (позаштатний) фахівців Із захисту інформації _____ (осіб)

4.5 Кількість фахівців, Які пройшли професійну підготовку
(Підвищення кваліфікації) в області інформаційної безпеки _____ (осіб)

5. Нормативна правова база та методичні документи щодо забезпечення безпеки інформації, які використовуються на підприємстві (перерахувати)

_____
_____
_____
_____

6. Наявність нормативних і організаційно-розпорядчих документів щодо захисту персональних даних (помітити):

		Так	Ні
6.1	Наказ про призначення структурного або посадової особи (працівника), відповідального за забезпечення безпеки персональних даних.		
6.2	Список осіб, доступ яких до персональних даних, оброблюваних в інформаційній системі, необхідний для виконання службових (трудових) обов'язків, затверджений керівником організації.		
6.3	Документи з обліку осіб, допущених до роботи з персональними даними в інформаційній системі.		
6.4	Документи з обліку застосовуваних засобів захисту інформації, експлуатаційної та технічної документації до них.		
6.5	Документи з обліку машинних носіїв персональних даних.		
6.6	Перелік персональних даних, що підлягають захисту.		
6.7	Акт класифікації інформаційної системи персональних даних.		
6.8	Приватна модель загроз і протокол експертної оцінки актуальності загроз.		
6.9	Вимоги щодо забезпечення безпеки персональних даних при обробці в інформаційних системах персональних даних.		
6.10	Порядок резервування та відновлення працездатності тех. засобів і програмного забезпечення, баз даних і систем захисту інформації.		
6.11	Порядок охорони приміщень.		
6.12	Положення по організації і проведенню робіт по забезпеченню безпеки персональних даних при їх обробці в інформаційній системі		
6.13	Посадові інструкції персоналу інформаційної системи персональних даних в частині забезпечення безпеки персональних даних при їх обробці в інформаційній системі персональних даних.		
6.14	Документи, що визначають порядок розгляду та складання висновків за фактами недотримання умов зберігання носіїв персональних даних, використання засобів захисту інформації, які можуть привести до порушення конфіденційності персональних даних або інших порушень, розробку і вживання заходів щодо запобігання можливих небезпечних наслідків подібних порушень.		
6.15	Документи, що визначають порядок припинення надання персональних даних у разі виявлення порушень порядку їх надання.		
6.16	Документи, що визначають порядок контролю за дотриманням умов використання засобів захисту інформації, передбачені експлуатаційної та технічної документації.		
6.17	Документи, що визначають умови розташування щодо кордонів контрольованої зони.		
6.18	Документи, що визначають конфігурацію і топологію інформаційної системи персональних даних, фізичних, функціональних та ін. зв'язків.		
6.19	Документи, що визначають перелік технічних засобів інформаційної системи персональних даних, загальносистемного та прикладного програмного забезпечення.		
6.20	Документи, що визначають режим обробки персональних даних в інформаційній системі персональних даних.		
6.21	Документи, що визначають ступінь участі персоналу в обробці персональних даних.		
6.22	Матриця доступу для інформаційної системи персональних даних.		
6.23	Документи, що визначають підрозділ (особа), відповідальна за експлуатацію засобів захисту інформації.		
6.24	Експлуатаційна документація на інформаційну систему та СЗІ, в тому числі антивірусного захисту: інструкція по встановленню та налагодженню адміністратору і користувачеві.		
6.25	Інструкція з організації парольного захисту.		
6.26	Акт встановлення та налаштування засобів захисту інформації.		
6.27	Акт за результатами приймально-здавальних випробувань засобів захисту інформації за результатами дослідної експлуатації.		

6.28	Висновок про можливість експлуатації засобів захисту інформації та перевірки їх готовності.		
6.29	Опис системи захисту персональних даних.		
6.30	Атестат відповідності забезпечення безпеки персональних даних		

7. Наявність організаційно-розпорядчих документів щодо захисту інформації в ключових системах інформаційної інфраструктури

		Так	Ні
7.1.	Про призначення відповідального за безпеку інформації в ключових системах інформаційної інфраструктури		
7.2	Визначення приналежності ключової системи інформаційної інфраструктури до одного з встановлених рівнів важливості.		
7.3	Визначення переліку ключової інформації в ключовий системі інформаційної інфраструктури.		
7.4	Оцінка наслідків порушень безпеки в ключовий системі інфраструктури.		
7.5	Аналіз і виявлення актуальних загроз безпеки інформації.		
7.6	Обґрунтування вимог щодо забезпечення безпеки інформації в ключовий системі інформаційної інфраструктури.		
7.7	Концепція забезпечення безпеки інформації в ключовий системі інформаційної інфраструктури.		
7.8	План заходів щодо забезпечення безпеки інформації в ключовий системі інформаційної інфраструктури.		
7.9	Включення ключовий системі інформаційної інфраструктури в реєстр ФСТЕК.		
7.10	Порядок залучення підрозділів організацій до розробки та розгортання системи забезпечення безпеки інформації або її елементів.		
7.11	Порядок тестування функцій систем захисту інформації від несанкціонованого доступу при зміні програмного середовища і персоналу автоматизованої системи за допомогою тест-програм, що імітують спроби несанкціонованого доступу.		
7.12	Наявність засобів відновлення системи захисту інформації від несанкціонованого доступу, які передбачають ведення двох копій програмних засобів системи захисту інформації від несанкціонованого доступу і їх періодичне оновлення і контроль працездатності.		
7.13	Порядок забезпечення цілісності програмних засобів системи захисту інформації від несанкціонованого доступу, а також незмінності програмного середовища.		
7.14	Журнал перевірки цілісності системи захисту інформації від несанкціонованого доступу при завантаженні системи по контрольних сумах.		
7.15	Прізвище та ім’я, тел. спеціаліста відповідального за безпеку інформації в ключових системах інформаційної інфраструктури.		

8. Наявність організаційно-розпорядчих документів щодо захисту конфіденційної інформації

		Так	Ні
8.1	Про призначення відповідального за технічний захист інформації		
8.2.	Про заборону обробки інформації обмеженого доступу на об'єктах інформатизації, неатестованих за вимогами забезпечення безпеки інформації		
8.3.	Про затвердження Положення про порядок організації та проведення робіт із захисту конфіденційної інформації		
8.4.	Про затвердження Переліку відомостей конфіденційного характеру		
8.5.	Про введення в дію атестованих об'єктів інформатизації		
8.6.	Атестат відповідності за вимогами забезпечення безпеки конфіденційної інформації		
8.7	Прізвище та ім’я, тел. спеціаліста відповідального за технічний захист інформації.		

9. Планування організаційно-технічних заходів щодо захисту інформації

		Так	Ні
9.1	Наявність плану організаційно-технічних заходів щодо захисту інформації за поточний рік.		
9.2	Наявність плану організаційно-технічних заходів щодо захисту інформації за минулий рік.		

9.3 Відсоток виконання плану організаційно-технічних заходів в поточному році ___%.
9.4 Відсоток виконання плану організаційно-технічних заходів в минулому році ___%.

10. Фінансування заходів з інформаційної безпеки

10.1 Середньорічна потреба у фінансуванні заходів інформаційної безпеки ____ (т.грн)
10.2 Реальне фінансування заходів з інформаційної безпеки за минулий і поточний рік _____ (тис.грн)

Керівник організації _____ _____
(Підпис) (П. І. Б.)
«___» _____ 20 __ р.

ДОДАТОК Б. Цілі заходів безпеки та заходи безпеки

Цілі заходів безпеки та заходи безпеки, наведені в Додатку, відповідають цілям заходів безпеки та сенсу безпеки, наведених в ISO/IEC 27001:2015 й мають використовуватися в процесі виконання Лабораторної роботи 6 – Контроль виконання заходів інформаційної безпеки.

A.5 Політики безпеки

A.5.1 Принципи управління інформаційною безпекою

Мета: Забезпечити принципи управління та підтримку інформаційної безпеки згідно з вимогами бізнесу та відповідними законами й нормативами.

A.5.1.1	Політики інформаційної безпеки	Заходи безпеки
		Набір політик щодо інформаційної безпеки повинен бути визначений, затверджений керівництвом, виданий і доведений до відома всього найманого персоналу та потрібних зовнішніх сторін
A.5.1.2	Перегляд політики інформаційної безпеки	Заходи безпеки
		Політики інформаційної безпеки потрібно переглядати в заплановані інтервали часу або за появи істотних змін для забезпечення їх постійної придатності, адекватності й ефективності

A.6 Організація інформаційної безпеки

A.6.1 Внутрішня організація

Мета: Визначити структуру управління для започаткування та контролю впровадження та функціонування інформаційної безпеки в організації

A.6.1.1	Ролі та обов’язки щодо інфор маційної безпеки	Заходи безпеки
		Усі обов’язки щодо інформаційної безпеки необхідно чітко визначити та розподілити
A.6.1.2	Розподіл обов’язків	Заходи безпеки
		Конфліктуючі обов’язки та сфери відповідальності мають бути розпо ділені для зменшення можливостей неавторизованої чи ненавмисної модифікації або неправильного використання ресурсів СУІБ організації
A.6.1.3	Контакти з повноважними органами	Заходи безпеки
		Необхідно підтримувати належні контакти з відповідними повноваж ними органами
A.6.1.4	Контакти з групами фахівцівз певної проблематики	Заходи безпеки
		Необхідно підтримувати належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об’єднаннями
A.6.1.5	Інформаційна безпека в управлінні проектами	Заходи безпеки
		Інформаційну безпеку потрібно брати до уваги під час управління проектами незалежно від типу проекту

А.6.2 Мобільне обладнання та віддалена робота

Мета: Гарантувати безпеку віддаленої роботи та використання мобільного обладнання.

А.6.2.1	Політика щодо мобільного обладнання	Заходи безпеки
		Політика та заходи підтримання безпеки мають бути пристосовані до управління ризиками, які виникають за рахунок використання мобільного обладнання
А.6.2.2	Віддалена робота	Заходи безпеки
		Політика та заходи підтримання безпеки мають бути запроваджені для захисту інформації, яка доступна, обробляється чи зберігається в місцях віддаленої роботи

А.7 Безпека людських ресурсів

А.7.1 Перед наймом

Національна примітка

Слово «найм» тут призначене, щоб охопити всі різноманітні ситуації: наймання людей (тимчасове чи постійне), призначення на посади, зміну посад, підписання контрактів та припинення дії будь-якої з цих угод.

Мета: Гарантувати, що найманий персонал та підрядники розуміють свої обов’язки, придатні до ролей, на які претендують.

А.7.1.1	Ретельна перевірка	Заходи безпеки
		Підтверджувальні перевірки біографічних даних усіх кандидатів на найм мають виконуватись згідно з усіма відповідними законами, нормативами та морально-етичними нормами, а також співвідносно до бізнес-вимог, класифікації інформації, до якої потрібен доступ, і усвідомлюваних ризиків
А.7.1.2	Терміни та умови найму	Заходи безпеки
		Контрактна угода з найманим персоналом та підрядниками має встановити взаємні відповідальності щодо інформаційної безпеки

А.7.2 Протягом найму

Мета: Впевнитися, що весь найманий персонал та підрядники усвідомлюють і виконують свої обов’язки з інформаційної безпеки.

А.7.2.1	Відповідальність керівництва	Заходи безпеки
		Керівництво повинно вимагати від найманого персоналу та підрядників застосування заходів безпеки згідно з установленими в організації політиками та процедурами
А.7.2.2	Поінформованість, освіта й навчання щодо інформаційної безпеки	Заходи безпеки
		Увесь найманий персонал організації, а там, де це суттєво, і підрядники повинні одержати належне навчання й тренінги для поінформованості та регулярно отримувати оновлені дані щодо політик і процедур організації, суттєвих для їх посадових функцій

A.7.2.3	Дисциплінарний процес	Заходи безпеки Має існувати формальний та офіційно оформлений дисциплінарний процес щодо найманого персоналу, який порушив інформаційну безпеку

A.7.3 Припинення чи зміна умов найму

Мета: Захистити інтереси організації як частини процесу зміни умов чи припинення найму.

A.7.3.1	Припинення чи зміна відповідальностей	Заходи безпеки Має бути чітко визначено, доведено до найманого персоналу чи підрядників і встановлено відповідальності за інформаційну безпеку та обов'язки, які залишаються дійсними після припинення чи зміни умов найму

A.8 Управління ресурсами СУІБ

A.8.1 Відповідальність за ресурси СУІБ

Мета: Ідентифікувати ресурси СУІБ організації і визначити відповідні обов'язки щодо їх захисту

A.8.1.1	Інвентаризація ресурсів СУІБ	Заходи безпеки Інформація, ресурси СУІБ, пов'язані з інформацією та обладнанням для обробки інформації, мають бути ідентифіковані та має підтримуватися їх актуальний інвентарний опис
A.8.1.2	Володіння ресурсами СУІБ	Заходи безпеки Ресурси СУІБ, які наявні в інвентарному описі, мають «бути у власності».
A.8.1.3	Припустиме використання ресурсів СУІБ	Заходи безпеки Правила щодо припустимого використання інформації та ресурсів СУІБ, пов'язаних із засобами оброблення інформації, мають бути ідентифіковані, задокументовані та впроваджені
A.8.1.4	Повернення ресурсів СУІБ	Заходи безпеки Увесь найманий персонал та користувачі зовнішньої сторони повинні повернути всі ресурси СУІБ організації, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди

А.8.2 Класифікація інформації

Мета: Забезпечити належний рівень захисту інформації відповідно до її важливості для організації.

А.8.2.1	Класифікація інформації	Заходи безпеки
		Інформація має бути класифікована в термінах правових вимог, її цінності, критичності й чутливості для неавторизованого розкриття чи модифікації
А.8.2.2	Маркування інформації	Заходи безпеки
		Має бути розроблено та впроваджено належну множину процедур для маркування й оброблення інформації згідно зі схемою класифікації, прийнятою організацією
А.8.2.3	Поводження з ресурсами СУІБ	Заходи безпеки
		Має бути розроблено та впроваджено процедури поводження з ресурсами СУІБ відповідно до схеми класифікації інформації, яку офіційно прийнято в організації

А.8.3 Поводження з носіями

Мета: Запобігти несанкціонованому розголошенню, модифікації, вилученню або знищенню інформації, яка зберігається на носіях.

А.8.3.1	Управління змінними носіями	Заходи безпеки
		Має бути впроваджено процедури управління змінними носіями відповідно до схеми класифікації, запровадженої в організації
А.8.3.2	Вилучення носіїв	Заходи безпеки
		Коли носії більше не потрібні, їх треба безпечно вилучати із застосуванням офіційно оформлених процедур
А.8.3.3	Фізичні носії під час передавання	Заходи безпеки
		Носії, що містять інформацію, має бути захищено від несанкціонова ного доступу, зловживання чи руйнування під час транспортування

А.9 Контроль доступу

А.9.1 Бізнес-вимоги до контролю доступу

Мета: Обмежити доступ до інформації та засобів оброблення інформації.

А.9.1.1	Політика контролю доступу	Заходи безпеки
		Політика контролю доступу має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки
А.9.1.2	Доступ до мереж та послуг мережі	Заходи безпеки
		Користувачі повинні отримувати доступ до мережі та послуг мережі лише тоді, коли вони були спеціально авторизовані для використання

А.9.2 Управління доступом користувача

Мета: Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.

А.9.2.1	Реєстрація та зняття з реєстрації користувача	Заходи безпеки
		Має бути впроваджено процес реєстрації та зняття з реєстрації для того, щоб була можливість управляти правами доступу
А.9.2.2	Забезпечення доступу користувачів	Заходи безпеки
		Має бути впроваджено формально затверджений процес забезпечення доступу користувачу для надання або вилучення прав доступу для всіх типів користувачів до всіх систем та послуг
А.9.2.3	Управління привілейованими правами доступу	Заходи безпеки
		Призначення та використання привілейованих прав доступу має бути обмежено та контрольовано
А.9.2.4	Управління таємною інформацією автентифікації користувачів	Заходи безпеки
		Облік таємної інформації автентифікації користувачів потрібно контролювати за допомогою офіційно оформленого процесу управління
А.9.2.5	Перегляд прав доступу користувача	Заходи безпеки
		Власники ресурсів СУІБ повинні переглядати права доступу користувача через регулярні встановлені інтервали
А.9.2.6	Вилучення або корекція прав доступу	Заходи безпеки
		Права доступу всього найманого персоналу та користувачів зовнішніх сторін до інформації та засобів оброблення інформації мають вилучатися після припинення найму, контракту чи угоди, або коректуватися після змін

А.9.3 Відповідальності користувача

Мета: Зробити користувачів відповідальними за збереження їх інформації автентифікації.

А.9.3.1	Використання таємної інформації автентифікації	Заходи безпеки
		Необхідно вимагати від користувачів додержання визначених в організації практик у використанні таємної інформації автентифікації

А.9.4 Контроль доступу до систем та прикладних програм

Мета: Запобігти несанкціонованому доступу до систем та прикладних програм.

А.9.4.1	Обмеження доступу до інформації	Заходи безпеки
		Доступ до інформації та функцій прикладних систем має бути обмежений відповідно до визначеної політики контролю доступу
А.9.4.2	Процедури безпечного підключення (log-on)	Заходи безпеки
		Доступ до систем та прикладних програм повинен контролювати процедурою безпечного підключення, коли це визначено політикою контролю доступу

A.9.4.3	Система управління паролем	Заходи безпеки
		Системи для управління паролями мають бути інтерактивними і забезпечувати якісні паролі
A.9.4.4	Використання привілейованих системних утиліт	Заходи безпеки
		Використання програм утиліт, що можуть бути спроможні скасовувати заходи безпеки системи та прикладних програм, має бути обмежено та суворо контрольовано
A.9.4.5	Контроль доступу до початкових кодів програм	Заходи безпеки
		Доступ до початкових кодів програм має бути обмежений

A.10 Криптографія

A.10.1 Криптографічні засоби захисту

Мета: Гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності та/або цілісності.

A.10.1.1	Політика використання криптографічних засобів	Заходи безпеки
		Має бути розроблено та впроваджено політику використання криптографічних засобів для захисту інформації
A.10.1.2	Управління ключами	Заходи безпеки
		Має бути розроблено та впроваджено політику використання, захисту й часу життя криптографічних ключів для всього їх життєвого циклу

A.11 Фізична безпека та безпека інфраструктури

A.11.1 Зони безпеки

Мета: Запобігти несанкціонованому фізичному доступу, пошкодженню та втручанню в її інформацію та засоби оброблення інформації.

A.11.1.1	Периметр фізичної безпеки	Заходи безпеки
		Для захисту зон, що містять конфіденційну або критичну інформацію чи засоби оброблення інформації, треба визначити та використовувати периметри безпеки
A.11.1.2	Заходи безпеки фізичного прибуття	Заходи безпеки
		Зони безпеки має бути захищено належними заходами безпеки прибуття, щоб гарантувати, що доступ дозволений лише персоналу, який отримав санкцію
A.11.1.3	Убезпечення офісів, кімнат та обладнання	Заходи безпеки
		Має бути розроблено й застосовано фізичну безпеку офісів, кімнат та обладнання
A.11.14	Захист від зовнішніх та інфраструктурних загроз	Заходи безпеки
		Має бути розроблено й застосовано фізичний захист від пошкодження внаслідок природних катакпізмів, акцій громадської непокори та аварій
A.11.1.5	Робота в зонах безпеки	Заходи безпеки
		Має бути розроблено та застосовано процедури роботи в зонах безпеки

А.11.1.6	Зони доставки та відвантаження	Заходи безпеки
		Щоб уникнути несанкціонованого доступу, має бути контрольовано й, за можливості, ізольовано від засобів оброблення інформації точки доступу, такі як зони доставки та відвантаження, а також інші точки, ерез які особи, доступ яких не санкціоновано, можуть увійти до службових приміщень

А.11.2 Обладнання

Мета: Запобігти втратам, пошкодженню, крадіжці або компрометації ресурсів СУІБ та перериванню діяльності організації.

А.11.2.1	Розміщення та захист обладнання	Заходи безпеки
		Обладнання має бути розміщено чи захищено так, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого несанкціонованого доступу
А.11.2.2	Допоміжні комунальні служби	Заходи безпеки
		Обладнання має бути захищено від аварійних відімкнень живлення та інших порушень, внаслідок аварій засобів життєзабезпечення
А.11.2 3	Безпека кабельних мереж	Заходи безпеки
		Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних послуг має бути захищено від перехоплювання, взаємного впливу чи пошкоджень
А.11.2.4	Обслуговування обладнання	Заходи безпеки
		Обладнання трібно правильно обслуговувати, щоб забезпечити його постійну доступність і цілісність
А.11.2.5	Переміщення майна	Заходи безпеки
		Обладнання, інформацію чи програмне забезпечення не потрібно виносити назовні без попередньої санкції на ці дії
А.11.2.6	Безпека обладнання та ресурсів СУІБ поза службовими приміщеннями	Заходи безпеки
		До ресурсів СУІБ поза службовими приміщеннями має бути застосов ний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації
А.11.2.7	Безпечне вилучення або повторне використання обладнання	Заходи безпеки
		Всі елементи обладнання, які містять носії пам'яті, має бути перевірено для забезпечення того, що будь-які конфіденційні дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення або повторного використання
А.11.2.8	Обладнання користувачів, залишене без нагляду	Заходи безпеки
		Всі елементи обладнання, які містять носії пам'яті, має бути перевірено для забезпечення того, що будь-які конфіденційні дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення або повторного використання
А.11.2.9	Політика чистого стола та чистого екрана	Заходи безпеки
		Повинні бути ухвалені політика чистого стола щодо паперів і змінних носіїв інформації та політика чистого екрана щодо засобів оброблення інформації

А.12 Безпека експлуатації

А.12.1 Процедури експлуатації та відповідальності

Мета: Забезпечити коректне та безпечне функціонування засобів оброблення інформації.

А.12.1.1	Документовані процедури експлуатації	Заходи безпеки
		Процедури експлуатації має бути задокументовано та зроблено доступними для всіх користувачів, що їх потребують
А.12.12	Управління змінами	Заходи безпеки
		Зміни в організації, бізнес-процесах, засобах оброблення інформації та системах, які впливають на інформаційну безпеку, мають бути контрольованими
А.12.1.3	Управління потужністю	Заходи безпеки
		Для забезпечення потрібної продуктивності системи необхідно здійснювати моніторинг та регулювати використання ресурсів і проектувати вимоги до майбутньої потужності
А.12.1.4	Відокремлення засобів розробки, тестування та експлуатації	Заходи безпеки
		Засоби розроблення, тестування та експлуатації має бути відокремлено для зменшення ризиків несанкціонованого доступу чи змін в операційному середовищі

А.12.2 Захист від зловмисного коду

Мета: Гарантувати, що інформація та засоби оброблення інформації захищені від зловмисного коду.

А.12.2.1	Заходи безпеки проти зловмисного коду	Заходи безпеки
		Має бути впроваджено заходи безпеки щодо виявлення, запобігання та відновлення для захисту від зловмисного коду і належні процедури поінформування користувачів

А.12.3 Резервне копіювання

Мета: Захистити від втрати даних

А.12.3.1	Резервне копіювання інформації	Заходи безпеки
		Згідно із затвердженою політикою резервного копіювання треба регулярно робити і в подальшому тестувати резервні копії інформації, програмного забезпечення та образів систем

А.12.4 Ведення журналів аудиту та моніторинг

Мета: Записувати події та генерувати докази.

А.12.4 1	Журнал аудиту подій	Заходи безпеки
		Журнал аудиту подій, у якому записується діяльність користувачів, винятки, збої та події інформаційної безпеки, треба вести, зберігати й регулярно переглядати
А.12.4.2	Захист інформації журналів реєстрації	Заходи безпеки
		Засоби реєстрування та інформація реєстрації має бути захищено від фальсифікації та несанкціонованого доступу
		Заходи безпеки

A.12.4.3	Журнали реєстрації адміністратора та оператора	Діяльність системного адміністратора та системного оператора має реєструватися і журнали аудиту мають бути захищені та регулярно переглядатися
A.12.4.4	Синхронізація годинників	Заходи безпеки Годинники всіх важливих систем оброблення інформації в організації або домені безпеки має бути синхронізовано з джерелом часу погодженої точності

A.12.5 Контроль програмного забезпечення, що перебуває в експлуатації

Мета: Гарантувати цілісність систем, що перебувають в експлуатації.

A.12.5.1	Інсталяція програмного забезпечення в системах, що перебувають в експлуатації	Заходи безпеки Мають бути наявними процедури контролю інсталяції програмного забезпечення в системах, що перебувають в експлуатації

A.12.6 Управління технічною вразливістю

Мета: Запобігати використанню технічних вразливостей.

A.12.6.1	Управління технічною вразливістю	Заходи безпеки Треба отримувати своєчасну інформацію щодо технічних вразливостей інформаційних систем, які використовують, оцінювати підвладність організації таким вразливостям і вживати належних заходів, щоб урахувати пов’язаний з цим ризик
A.12.6.2	Обмеження на інсталяцію програмного забезпечення	Заходи безпеки Має бути розроблено та впроваджено правила стосовно інсталяції програмного забезпечення користувачами

A.12.7 Розгляд аудиту інформаційних систем

Мета: Мінімізувати вплив аудиту на системи, які перебувають у промисловій експлуатації.

A.12.7.1	Заходи безпеки аудиту інформаційних систем	Заходи безпеки Вимоги аудиту та діяльність, що охоплює перевірки систем, які пере бувають в експлуатації, має бути ретельно сплановано та погоджено, щоб мінімізувати ризик порушення бізнес-процесів

А.13 Безпека комунікацій

А.13.1 Управління безпекою мережі

Мета: Забезпечити захист інформації в мережах та захист засобів оброблення інформації, що їх підтримує

А.13.1.1	Заходи безпеки мережі	Заходи безпеки
		Треба відповідним чином управляти й захищати мережі для захисту інформації в системах і прикладних програмах
А.13.1.2	Безпека послуг мережі	Заходи безпеки
		Характеристики безпеки, рівні послуг, а також вимоги управління всіма послугами мережі має бути ідентифіковано і міститися в будь-якій угоді щодо послуг мережі як для послуг, які надає сама організація, так і для аутсорсингових послуг
А.13.1.3	Сегментація в мережах	Заходи безпеки
		У мережі мають бути сегментовані групи інформаційних послуг, користувачів, а також інформаційні системи

А.13.2 Обмін інформацією

Мета: Підтримувати безпеку інформації, якою обмінюються всередині організації та з зовнішнім об’єктом.

А.13.2.1	Політики та процедури обміну інформацією	Заходи безпеки
		Мають бути наявними офіційно оформлені політики, процедури та заходи безпеки для захисту обміну інформацією з використанням усіх видів засобів комунікації
А.13.2.2	Угоди щодо обміну інформацією	Заходи безпеки
		Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо безпечного обміну бізнес-інформацією
А.13.2.3	Електронний обмін повідомленнями	Заходи безпеки
		Інформація, яка міститься в електронних повідомленнях, має бути захищена належним чином
А.13.2.4	Угоди щодо конфіденційності або нерозголошення	Заходи безпеки
		Вимоги до угод щодо конфіденційності або нерозголошення, які відображують потреби організації в захисті інформації, мають бути ідентифіковані, задокументовані та регулярно переглядатися

А.14 Придбання, розроблення та підтримка інформаційних систем

А.14.1 Вимоги щодо безпеки для інформаційних систем

Мета: Гарантувати, що безпека є невід'ємною частиною інформаційних систем протягом всього життєвого циклу Це також включає вимоги для інформаційних систем, які забезпечують надання послуг з використанням публічних (загальнодоступних) мереж.

А.14.1.1	Аналіз та специфікація вимог інформаційної безпеки	Заходи безпеки
		Вимоги щодо інформаційної безпеки має бути долучено в положення щодо бізнес-вимог до нових інформаційних систем або модернізацій до наявних інформаційних систем
А.14.1.2	Безпечні прикладні сервіси в публічних мережах	Заходи безпеки
		Інформація в прикладних сервісах, яку передають через публічні мережі, має бути захищеною від шахрайської діяльності, контрактних суперечок, несанкціонованого розголошення та модифікації
А .14.1.3	Захист транзакцій прикладних сервісів	Заходи безпеки
		Інформація, залучена в транзакції прикладних сервісів, має бути захищена для запобігання неповній передачі, неправильній маршрутизації, несанкціонованій зміні повідомлення, несанкціонованому розголошенню, несанкціонованому дублюванню повідомлення чи його повторенню

А.14.2 Безпека в процесах розроблення та підтримки

Мета: Гарантувати, що інформаційну безпеку проектують та впроваджують протягом життєвого циклу розроблення інформаційних систем.

А.14.2.1	Політика безпечного розроблення	Заходи безпеки
		Потрібно встановлювати та застосовувати до розробників всередині організації правила для розроблення програмного забезпечення та систем
А.14.2.2	Процедури контролю змін системи	Заходи безпеки
		Зміни в системах всередині життєвого циклу розроблення мають бути контрольованими за допомогою офіційно оформлених процедур контролю змін
А.14.2.3	Технічний перегляд прикладних програм після змін операційної платформи	Заходи безпеки
		Коли операційні платформи змінено, критичні для бізнесу прикладні програми має бути переглянуто й протестовано, щоб забезпечити відсутність негативного впливу на функціонування та безпеку організації
А.14.2.4	Обмеження на зміни до пакетів програмного забезпечення	Заходи безпеки
		Модифікації пакетів програмного забезпечення не повинні заохочуватися, бути обмеженими найнеобхіднішими змінами і всі зміни потрібно суворо контролювати
А.14.2.5	Принципи проектування безпечної системи	Заходи безпеки
		Принципи проектування безпечних систем потрібно розробити, задокументувати, виконувати та

		використовувати для будь-яких зусиль щодо реалізації інформаційних систем
A.14.2.6	Безпечне середовище роз- роблення	Заходи безпеки
		Організації повинні запровадити та відповідним чином захистити безпечне середовище проектування для розроблення систем та інтеграції зусиль, що покривають повний життєвий цикл розроблення системи
A.14.2.7	Аутсорсингове розроблення	Заходи безпеки
		Організація повинна здійснювати нагляд над аутсорсинговим розробленням систем та його моніторинг
A.14.2.8	Тестування безпеки системи	Заходи безпеки
		Тестування функціональності безпеки потрібно виконувати протягом розроблення
A.14.2.9	Приймальне тестування системи	Заходи безпеки
		Програми приймального тестування та відповідні критерії має бути визначено для нових інформаційних систем, оновлень та нових версій

A.14.3 Дані для тестування системи

Мета: Забезпечити захист даних, які використовують для тестування.

A.14.3.1	Захист даних для тестування системи	Заходи безпеки
		Дані для тестування має бути ретельно відібрано, захищено та контрольовано

A.15 Взаємовідносини з постачальниками

A.15.1 Інформаційна безпека у взаємовідносинах з постачальниками

Мета: Гарантувати захист ресурсів СУІБ організації, які можуть бути доступні постачальникам.

A.15.1.1	Політика інформаційної безпеки для взаємовідносин з постачальниками	Заходи безпеки
		Вимоги інформаційної безпеки для послаблення ризиків, пов’язаних із доступом постачальників до ресурсів СУІБ організації має бути погоджено з постачальником та задокументовано
A.15.1.2	Врахування безпеки в угодах з постачальниками	Заходи безпеки
		Усі відповідні вимоги щодо інформаційної безпеки має бути встановлено та погоджено з кожним постачальником, який може мати доступ, обробляти, зберігати, передавати чи надавати компоненти ІТ-інфраструктури для інформації організації
A.15.1.3	Ланцюг постачання інформаційних та комунікаційних технологій	Заходи безпеки
		Угоди з постачальниками мають містити вимоги стосовно адресації ризиків інформаційної безпеки, пов’язаних з ланцюгом постачання продуктів та послуг інформаційних і комунікаційних технологій

А.15.2 Управління наданням послуг постачальником

Мета: Підтримувати належний рівень інформаційної безпеки та надання послуг відповідно до угод з постачальниками.

А.15.2.1	Моніторинг та перегляд по слуг постачальника	Заходи безпеки
		Організація повинна регулярно проводити моніторинг, перегляд та аудит отримання послуг постачальника
А.15.2.2	Управління змінами у послугах постачальника	Заходи безпеки
		Зміни в наданні послуг постачальника, зокрема й підтримування та вдосконалювання наявних політик інформаційної безпеки, процедур і заходів безпеки, мають управлятися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків

А.16 Управління інцидентами інформаційної безпеки

А.16.1 Управління інцидентами інформаційної безпеки та вдосконаленням

Мета: Гарантувати послідовний та ефективний підхід до управління інцидентами інформаційної безпеки, охоплюючи поширення інформації про події безпеки та слабкі місця.

А.16.1.1	Відповідальності та процедури	Заходи безпеки
		Має бути визначено відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки
А.16.1.2	Звітування про події інформаційної безпеки	Заходи безпеки
		Необхідно якнайшвидше звітувати стосовно подій інформаційної безпеки через належні канали управління
А .16.1.3	Звітування щодо слабких місць інформаційної безпеки	Заходи безпеки
		Треба вимагати від усього найманого персоналу та підрядників, які користуються інформаційними системами та послугами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць у системах чи послугах
А.16.1.4	Оцінювання та прийняття рішення стосовно подій інформаційної безпеки	Заходи безпеки
		Події інформаційної безпеки має бути оцінено та прийнято рішення стосовно віднесення їх до інцидентів інформаційної безпеки
А.16.1.5	Реагування на інциденти інформаційної безпеки	Заходи безпеки
		Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до задокументованої процедури
А.16.1.6	Знання з вивчення інцидентів інформаційної безпеки	Заходи безпеки
		Знання, отримані з аналізу та розв’язання інцидентів інформаційної безпеки, мають використовуватися для зменшення ймовірності чи впливу майбутніх інцидентів
А.16.1.7	Збирання доказів	Заходи безпеки
		Організація повинна визначити і використовувати процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази

A.17 Аспекти інформаційної безпеки управління безперервністю бізнесу

A.17.1 Безперервність інформаційної безпеки

Мета: Безперервність інформаційної безпеки має бути залучено в системи управління безперервністю бізнесу організації.

A.17.1.1	Планування безперервності інформаційної безпеки	Заходи безпеки
		Організація повинна визначити свої вимоги щодо інформаційної безпеки та безперервності управління інформаційною безпекою в надзвичайних ситуаціях, наприклад під час кризи чи катастрофи

A.17.1.2	Реалізація безперервності інформаційної безпеки	Заходи безпеки
		Організація повинна розробити, задокументувати, реалізувати та підтримувати процеси, процедури та заходи безпеки для гарантування необхідного рівня безперервності щодо інформаційної безпеки під час надзвичайної ситуації
A.17.1.3	Верифікація, перегляд та оцінювання безперервності інформаційної безпеки	Заходи безпеки
		Організація повинна підтверджувати розроблені та впроваджені за ходи безперервності інформаційної безпеки через регулярні інтерва ли часу для гарантування, що вони дійсні та ефективні протягом надзвичайних ситуацій

A.17.2 Резервне обладнання

Мета: Гарантувати доступність обладнання для оброблення інформації.

A.17.2.1	Доступність обладнання для оброблення інформації	Заходи безпеки
		Обладнання оброблення інформації має бути впроваджено з резервуванням, достатнім для того, щоб відповідати вимогам доступності

A.18 Відповідність

A.18.1 Відповідність правовим та контрактним вимогам

Мета: Уникнути порушень будь-якого закону, вимог, що діють на підставі закону, нормативних або контрактних зобов’язань, пов’язаних з інформаційною безпекою та будь-якими вимогами щодо безпеки.

A.18.1.1	Ідентифікація застосовного законодавства та контракт них вимог	Заходи безпеки
		Усі важливі вимоги, що діють на підставі закону, нормативні чи контрактні вимоги та підхід організації до задоволення цих вимог має бути чітко визначено, задокументовано та актуалізовано для кожної інформаційної системи та організації
A.18.1.2	Права	Заходи безпеки

	інтелектуальної власності	Має бути впроваджено належні процедури забезпечення відповідності законодавчим, нормативним і контрактним вимогам щодо прав інтелектуальної власності та щодо використання запатентованих продуктів програмного забезпечення
A.18.1.3	Захист організаційних записів	Заходи безпеки Відповідно до законодавчих, регуляторних, контрактних і бізнес-вимог важливі записи має бути захищено від втрати, знищення, фальсифікації, несанкціонованого доступу та несанкціонованого використання
A.18.1.4	Захист даних та конфіденційність персональних даних	Заходи безпеки Конфіденційність і захист даних, що ідентифікують особу, має бути забезпечено згідно з вимогами відповідного законодавства та регуляторними вимогами, за наявності
A.18.1.5	Нормативи щодо криптогра фічних засобів	Заходи безпеки Криптографічні засоби потрібно використовувати відповідно до всіх застосовних угод, законів та регуляторних вимог

A .18.2 Перевірки інформаційної безпеки

Мета: Гарантувати, що інформаційна безпека впроваджена та працює відповідно до організаційних політик та процедур.

A.18.2.1	Незалежні перевірки інформаційної безпеки	Заходи безпеки Підходи організації до управління інформаційною безпекою та її впровадження (тобто цілі заходів безпеки, заходи безпеки, політики, процеси й процедури для інформаційної безпеки) мають незалежно перевірятися через заплановані інтервали або коли відбуваються значні зміни
A.18.2.2	Відповідність політикам і стандартам безпеки	Заходи безпеки Керівники повинні регулярно перевіряти відповідність оброблення інформації та процедур у межах сфери їх відповідальності належним політикам, стандартам та іншим вимогам щодо безпеки
A.18.2.3	Перевірка технічної відповід ності	Заходи безпеки Інформаційні системи потрібно регулярно перевіряти на відповідність політикам і стандартам інформаційної безпеки організації

ДОДАТОК В. Вимоги до оформлення звітів

Основний текст оформлюється у наступному стилі:

- шрифт Times New Roman текстового редактора Word;
- кегль – 14 п.;
- полуторний міжрядковий інтервал;
- вирівнювання по ширині;
- абзацний відступ 1см.

В якості графічних матеріалів можуть бути застосовані копії екранів, що підтверджують працездатність розробок та наявність результатів, ілюстрації, таблиці (якщо є необхідність розміщення не повної талиці, а її частки, скрину), графіки, діаграми тощо.

Оформлення графічного матеріалу: по центру, без абзацного відступу; назва – також по центру, без абзацного відступу. Графічний матеріал відокремлюється від основного тексту роботи порожнім рядком – до та після назви рисунку. На графічний матеріал слід робити посилання (наприклад, «на рисунку 2 відображено…»).

Таблицю, як і ілюстрацію, слід розташовувати безпосередньо після тексту, у якому вона згадується вперше або на наступній сторінці. На всі таблиці мають бути посилання в тексті звіту.

Таблиці нумеруються арабськими цифрами порядковою нумерацією в межах звіту. Таблиця повинна мати назву, яку друкують малими літерами (крім першої великої) і розміщують над таблицею. Назва має бути стислою і відбивати зміст таблиці.

Таблицю з великою кількістю рядків можна переносити на наступну сторінку. При перенесенні таблиці на наступну сторінку назву вміщують тільки над її першою частиною. Слово “Таблиця __” вказують один раз зліва над першою частиною таблиці, над іншими частинами пишуть: « Продовження таблиці __». В таблицях допустимо зменшення розміну шрифту та встановлення однарного міжрядкового інтервалу.

Частини програмного коду надаються з поясненнями й у наступному стилі: шрифт Times New Roman, кегль – 10 п.; одинарний міжрядковий інтервал; вирівнювання вліво; абзацний відступ 1см.

Вимоги до викладення матеріалів звіту з виконання лабораторних робіт. У звіті до роботи повинно бути наведено.

1. Титул
2. Мета роботи

3 Головна частина з описом об’єкту дослідження та оглядом сфери застосування.

4. Покроковий опис виконання завдань з копіями екранів, що підтверджують отримання результатів.
5. Висновки
6. Перелік застосованих джерел

ДОДАТОК Г. Приклад оформлення титульного листа

ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
Факультет комп’ютерно-інформаційних технологій та автоматизації
Кафедра прикладної математики і інформатики

ЗВІТ З ВИКОНАННЯ ІЛАБОРАТОРНОЇ РОБОТИ

з дисципліни «Інформаційна безпека»
за темою: «_____»

Виконав:

Студент (-тка) гр. _____

_____ _____

(дата, підпис) (ПІБ)

Перевірив:

_____ _____

(дата, підпис) (ПІБ)

20__