Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет_Інформаційних радіотехнологій та технічного захисту інформації

Кафедра_Комп'ютерної радіоінженерії та систем технічного захисту інформації_

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
_____Організаційний захист електронних інформаційних_____.
_____ресурсів на підприємстві _____.
(тема)

Виконав:
студент _2_ курсу, групи __СТЗІАм-22-1____
_____Кулько П.О._____
(прізвище, ініціали)

Спеціальність _____125_____
_____Кібербезпека_____

Тип програми ____освітньо-професійна _____

Освітня програма ___Системи технічного____
захисту інформації, автоматизація її обробки

Керівник _____проф. Милютченко І.О._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Антіпов І.Є.
(підпис)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій та технічного захисту інформації
Кафедра Комп'ютерної радіоінженерії та систем технічного захисту інформації
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
Тип програми освітньо-професійна
Освітня програма Системи технічного захисту інформації, автоматизація її обробки

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Кульку Петру Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Організаційний захист електронних інформаційних ресурсів на підприємстві
затверджена наказом університету від 03 11 2023 р. № 1281 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 10 01 2024 р.
3. Вихідні дані до роботи Виконати аналіз поняття електронних інформаційних ресурсів (EIP) та їх класифікації. Розробити заходи організаційного захисту EIP на підприємстві за напрямами: режим охорони, робота зі співробітниками, робота з документами, використання технічних засобів, аналіз загроз, контроль ресурсів обмеженого доступу тощо. Розробити структуру та функції служби захисту інформації. Сфера діяльності підприємства – розробка освітніх інструментів для українських та закордонних платформ

4. Перелік питань, що потрібно опрацювати в роботі
1 Поняття, визначення та класифікація IP та EIP. 2 Структура IP та EIP підприємства. 3 Опис моделей загроз інформації та порушника 4 Методи та засоби організаційного захисту EIP. 5 Політика безпеки інформації. Висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

1. Класифікація ІР.
2. Класифікація EIP.
3. Структура ІР підприємства.
4. Модель можливих загроз.
5. Модель порушника..
6. Порівняння електронного та власноручного підпису
7. Модель верифікації облікових даних (Verifiable credentials)
8. Політика безпеки інформації.
9. Засоби захисту ПЗ підприємства.
10. Структура та завдання служби захисту інформації підприємства

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Огляд літератури	06.11 - 12.11	
2	Аналіз поняття і класифікації EIP	13.11 - 19.11	
3	Формування структури EIP на підприємстві	20.11 - 26.11	
4	Розробка моделі загроз та порушника	27.11 - 03.12	
5	Обгрунтування заходів організаційного захисту	04.12 - 17.12	
6	Формування політики захисту інформації на	18.12 - 24.12	
	підприємстві		
7	Оформлення графічних матеріалів та	25.12 - 31.12	
	записки		
8	Подання на рецензування та антиплагіатну	01.01 - 10.01	

Дата видачі завдання __10_ _____10___ 2023 р.

Студент _____
(підпис)

Керівник роботи _____ ___проф. Милютченко І.О.___
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 69 с., 7 рис., 7 табл., 2 додатки, 28 джерел.

ІНФОРМАЦІЙНІ РЕСУРСИ, ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ, ВЕРІФІКАЦІЯ ОБЛІКОВИХ ДАНИХ, ЕЛЕКТРОННІ ПІДПИСИ, ВЛАСНОРУЧНІ ПІДПИСИ.

Об’єкт дослідження – електронні інформаційні ресурси.

Предмет дослідження – система захисту електронних інформаційних ресурсів на підприємстві.

У кваліфікаційній роботі розглянуто визначення інформаційних ресурсів, електронних інформаційних ресурсів, їх структура, засоби захисту електронних ресурсів від несанкціонованого доступу та засоби технічного захисту інформації. Проведений аналіз щодо використання електронних підписів, підходу з моделлю верифікації облікових даних (Verifiable credentials), бази даних. Розглянуто підприємство, яке розробляє освітні проекти, проведений аналіз можливих каналів витоків інформації.

Галузь використання – системи технічного захисту інформації.

ABSTRACT

Explanatory note of qualification work: 69 p., 7 fig., 7tab., 2 application, 28 sources.

INFORMATION RESOURCES, ELECTRONIC INFORMATION RESOURCES, VERIFICATION OF ACCOUNT DATA, ELECTRONIC SIGNATURES, MANUAL SIGNATURES.

Object of study – electronic information resources.

Subject of study – a system for protecting electronic information resources at the enterprise.

The qualification work considers the definition of information resources, electronic information resources, their structure, means of protecting electronic resources from unauthorized access, and means of technical information protection. The analysis of the use of electronic signatures, the approach with the verification model of credentials (Verifiable credentials), and databases was carried out. An enterprise that develops educational projects was considered, and an analysis of possible channels of information leaks was carried out.

Sphere of use – systems of technical protection of information.

ПЕРЕЧЕНЬ СКОРОЧЕНЬ ТА АБРЕВІАТУР

АС – Автоматизована система

БД – База даних

ДІР – Державні інформаційні ресурси

ІР – Інформаційні ресурси

ЕІР – Електронні інформаційні ресурси

ЕП – Електронний підпис

КЕП – Кваліфікований електронний підпис

КСЗІ – Комплексна система захисту інформації

ПЗ – Програмне забезпечення

СЗІ – Служба захисту інформації

СУБД – Система управління базою даних

ТД – Технічна документація

VC – Verifiable credentials (верифіковані облікові дані)

ЗМІСТ

ВСТУП

У сучасному світі інформаційні ресурси відіграють надзвичайно важливу роль у функціонуванні підприємств та організацій різних масштабів. Забезпечення безпеки цих ресурсів, зокрема електронних інформаційних ресурсів, стає важливим завданням для будь-якого сучасного підприємства. Для досягнення цієї мети необхідно ретельно вивчати концепції, визначення та класифікацію інформаційних ресурсів та електронних інформаційних ресурсів.

У сучасному цифровому світі поняття «інформаційні ресурси» займає центральне місце, визначаючи ефективність і результативність діяльності як суспільних структур, так і підприємств. З ростом обсягів цифрової інформації та її значущості для забезпечення безпеки та ефективного використання, управління та захист інформаційних ресурсів стає критично важливим завданням.

Важливим є осмислення різноманітності інформаційних ресурсів, їх класифікації, а також вивчення місця та ролі електронних інформаційних ресурсів у сучасному інформаційному просторі. Зокрема, дослідження важливості управління інформаційними ресурсами для ефективного функціонування підприємств у сучасному економічному середовищі. Вивчення баз даних та технічної документації, а також визначення можливих загроз для інформації та методів захисту, допомагає зрозуміти складність та важливість питань інформаційної безпеки.

Доцільним є розгляд електронних підписів та використання верифікованих облікових даних (Verifiable credentials) як сучасних інструментів для забезпечення цілісності та автентичності цифрових документів.

Дослідження, проведене у даній роботі, має на меті висвітлити значення та вплив інформаційних ресурсів на сучасне суспільство, а також виявити ефективні шляхи їх управління та захисту для забезпечення безпеки та ефективного використання інформації у різних сферах діяльності.

Апробація результатів, розглянутих у кваліфікаційній роботі, відбулася в рамках 27-го Міжнародному Молодіжного Форуму «Радіоелектроніка і молодь у XXI столітті».

1 ПОНЯТТЯ, ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ ІР ТА ЕІР

Зважаючи на важливість ефективного управління інформацією в сучасному цифровому світі, поняття, визначення та класифікація інформаційних ресурсів (ІР) та електронних інформаційних ресурсів (ЕІР) стають ключовими аспектами для розвитку та забезпечення безпеки даних у різних сферах діяльності. Доцільно розглядати поняття ІР та їх класифікацію з урахуванням сучасних вимог та тенденцій у сфері цифрової безпеки. Важливими для розгляду є особливості ЕІР, їх значення та вплив на сучасні організаційні процеси.

1.1 Інформаційні ресурси

Нині в науковому та суспільному просторі поряд з традиційним поняттям «ресурси» важливим є поняття «інформаційні ресурси», яке визначають, зокрема, як систематизовану сукупність документів, зафіксованих на паперових чи інших носіях, в інформаційних системах [1].

У контексті ХХ століття ресурси були класифіковані як матеріальні, енергетичні, трудові, фінансові та технологічні. Однак, починаючи з кінця 70-х років, виникла необхідність в розгляді ІР як окремої категорії. Ці ресурси функціонують незалежно та володіють унікальними властивостями, суттєво впливаючи на всі сфери суспільних процесів [2].

Розширення та ускладнення засобів, методів і форм автоматизації обробки інформації призводить до збільшення залежності суспільства від рівня безпеки інформаційних технологій, що використовуються у всіх сферах людської та суспільної діяльності. Концепція розвитку сектору безпеки і оборони України включає в себе «впровадження сучасних інформаційних технологій в систему управління та забезпечення захисту інформаційних ресурсів, а також формування

та реалізацію державної політики у сфері кіберзахисту державних електронних інформаційних ресурсів» [3].

Ефективний вибір методів та засобів захисту залежить від характеру та призначення ІР. Таким чином, актуальною є проблема визначення терміну «інформаційний ресурс» та ознак його класифікації в різних контекстах, таких як національна безпека, інформаційні технології, документно-комунікаційні системи, суспільство, бібліотекознавство та інше [3].

Однак визначення терміну «інформаційні ресурси» розрізняється в залежності від сфери застосування, що підтверджує відсутність єдиного та загальноприйнятого визначення. Є різноманітні тлумачення в контексті національної безпеки, економіки, бібліотекознавства тощо [3].

Класифікація ІР відбувається за різними ознаками, які залежать від характеру та значення ІР, режиму доступу тощо. Аналіз ознак та видів ІР показує подібний зміст різних формулювань та деяке повторення в різних ознаках [3].

У контексті норм Закону України «Про науково-технічну інформацію» [4], ІР визначаються як систематизовані довідково-інформаційні фонди, які мають відповідний довідково-пошуковий апарат та технічні засоби для зберігання, обробки та передачі. Ці ІР знаходяться в управлінні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій [2].

Однак, більш загальноприйнятим визначенням є концепція ІР як сукупності документів у різноманітних інформаційних системах, таких як бібліотеки, архіви, банки даних та інші. Це поняття знайшло своє закріплення в Національній програмі інформатизації та в Законі «Про бібліотеки і бібліотечну справу» [2].

Українське законодавство, на жаль, не надає єдиного визначення правового режиму ІР, а замість цього, встановлює правові норми для регулювання їх функціонування в окремих інформаційних системах. Визначення ІР згідно з уніфікованими державними стандартами та нормами включає у себе

систематизоване зібрання документів на паперових або інших носіях інформації, а також сукупність даних, призначених для забезпечення ефективного отримання достовірної інформації. У разі ІР науково-технічної інформації, це охоплює систематизоване зібрання науково-технічної літератури та документації, що включає книги, брошури, періодичні видання, патентну документацію, нормативно-технічну документацію тощо [2].

У контексті спільного користування, ІР включають в себе державні органи науково-технічної інформації, наукові та науково-технічні бібліотеки, комерційні центри, фірми та організації, що здійснюють науково-технічну діяльність та мають угоди про спільне використання ІР [2].

Правовий режим ІР складається з комплексу правових норм, які визначають процедури власності на інформацію, процедури документування, рівні доступу до інформації, механізми захисту інформації, а також права учасників інформаційних відносин стосовно конкретного ІР [2].

Визначення поняття «інформаційні ресурси», наведене у конспекті лекцій «Основи інформаційної безпеки» Заплотинського Б.А., науковець досить точно описує поняття в контексті інформаційної безпеки та управління інформацією: «Інформаційні ресурси – це окремі документи та масиви документів, представлені самостійно або в інформаційних системах (бібліотеках, архівах, фондах, базах даних та інших ІР).» [5]. Згідно визначення науковця, ІР можуть включати в себе як окремі документи, такі як текстові файли, таблиці, презентації тощо, так і більш об’ємні масиви документів, які можуть бути частиною більшого набору інформації. Науковець акцентує увагу на тому, що ІР можуть приймати різні форми і знаходитися в різних місцях, також можуть бути надзвичайно цінними для організацій та осіб, тому важливо ефективно керувати та захищати їх для збереження інформаційної безпеки.

Низенко Е. І., Каленяк В. П. у своїй роботі «Забезпечення інформаційної безпеки підприємництва» [6] виокремлюють поняття «інформаційних ресурсів», як

«інформація з обмеженим доступом, що становить банківську і комерційну таємниці; інформація, віднесена до категорії державної таємниці, конфіденційна інформація тощо.». Ця дефініція вказує на важливість аспекту інформаційної безпеки, у контексті збереження конфіденційності ІР державних та підприємських установ. Науковці підкреслюють значущість інформаційної безпеки у сфері підприємства. Захист ІР, зокрема конфіденційних і цінних даних, є важливою частиною діяльності підприємств для забезпечення їхнього успішного функціонування і запобігання можливим ризикам та загрозам з боку зловмисників.

Поняття «інформаційні ресурси спільного користування» визначається як сукупність ІР, що об'єднують державні органи, науково-технічні бібліотеки, а також комерційні центри, фірми та організації, що активно займаються науково-технічною діяльністю. Ця група суб'єктів укладає договори, регулюючи спільне використання ІР, включаючи доступ до державних органів науково-технічної інформації та відповідних бібліотек [7].

Інша категорія, «інформаційні ресурси науково-технічної інформації», складається з методично зібраної науково-технічної літератури та документації, що включає різноманітні види видань, такі як книги, брошури, періодичні видання, патентна та нормативно-технічна документація, а також звітна науково-технічна документація, що виникає в процесі наукових та дослідно-конструкторських робіт. Ці матеріали зафіксовані на паперових та інших носіях [7].

Варто відзначити, що найбільш універсальне визначення поняття «інформаційний ресурс» міститься у Законі України «Про національну програму інформатизації» [8]. Відповідно до статті 1 цього Закону, ІР є сукупністю документів, які зберігаються в інформаційних системах, таких як бібліотеки, архіви, банки даних та інші аналогічні структури. Ця визначення забезпечує обґрунтування відносин між ІР та інформаційними системами, підкреслюючи ключову роль останніх у зберіганні та обробці документів [7].

Для докладного розуміння змісту ІР, доцільно розглянути їх класифікацію.

Згідно з упередженою класифікацією ресурсів, перший аспект визначає їх матеріальність. Він об'єднує матеріальні ресурси, які можуть бути використані за необхідності, та ресурси обчислювальних систем, що включають компоненти, які дозволяють обробляти дані на певний проміжок часу [2]. Крім того, ресурси можуть бути розділені на загальнодоступні та захищені, залежно від ступеня обмеженості доступу до них. Зокрема, захищені ресурси електронних-обчислювальних машин (ЕОМ) вимагають спеціального ключа секретності для контролю доступу [2].

Особливий акцент робиться на ІР, які можуть мати кілька визначень. По-перше, це об'єктивне відображення закономірностей та фактів у суспільстві та природному середовищі, що є науковими знаннями, зафіксованими у довідково-інформаційних фондах та бібліотеках. Друге визначення включає окремі документи та масиви документів у системах інформації, що містять різноманітні дані з усіх сфер суспільного життя. Третє визначення вказує на значущі дані для підприємства, такі як матеріальні ресурси, а також основні та допоміжні масиви в зовнішній пам'яті комп'ютерних систем і вхідні документи [2].

Подальша класифікація ІР базується на кількох ознаках, включаючи вид інформації, вид носія, режим доступу, спосіб організації зберігання та використання, спосіб формування та розповсюдження, а також форму власності. За видом інформації, ІР можуть містити дані різних напрямків, таких як:

- правові,
- науково-технічні,
- політичні,
- економічні,
- соціальні,
- медичні тощо.

Залежно від носія, вони можуть бути відображені на папері, машиночитаних носіях, у вигляді зображення на екрані ЕОМ, в пам'яті комп'ютерних систем, каналах зв'язку та інших носіях. Ресурси також можуть бути класифіковані за режимом доступу, що відображає відкриті або обмежені ступені доступу до інформації [2].

Класифікація ІР залежно від способу їх організації зберігання та використання демонструє наявність двох основних форм: традиційні та автоматизовані форми. Традиційні форми організації включають масиви документів, фонди документів та архіви, що активно використовуються для зберігання та доступу до інформації. У той же час, автоматизовані форми, такі як бази даних та інформаційні автоматизовані системи, набувають все більшої популярності в сучасному інформаційному середовищі [2].

Подальша класифікація ІР за способом їх формування та розповсюдження розкриває два основних стани: стаціонарний та рухомий. Це вказує на те, що ІР можуть перебувати в стаціонарних місцях, таких як бібліотеки, архіви чи інші організаційні структури, або бути в рухомому стані, що означає можливість доступу до них у будь-який час та в будь-якому місці [2].

Нарешті, класифікація ІР за формою власності підкреслює їх правовий статус. Ця класифікація розрізняє ресурси як загальнодержавне національне надбання, державну, муніципальну, приватну та колективну власність, що вказує на різноманітність правових відносин, пов'язаних з володінням та управлінням інформаційними ресурсами [2].

Зазначена класифікація ІР відображає різноманітність їх організаційних, функціональних та правових аспектів, що важливо для належного розуміння та ефективного використання ІР у різних сферах діяльності [2].

Згідно Закону України «Про Державну службу спеціального зв’язку та захисту інформації» поняття «державні інформаційні ресурси» це «інформація, яка є власністю держави та необхідність захисту якої визначено законодавством» [9].

Це визначення вказує, що інформація яка належить державі або керується нею, є державними ІР. Ці ресурси можуть включати в себе різні види інформації, яка використовується органами державної влади та іншими державними установами для виконання їхніх функцій та завдань. Згідно з Законом, державні ІР мають високий ступінь важливості для держави та суспільства і, отже вони потребують особливого захисту. Цей захист може включати в себе заходи для збереження конфіденційності, цілісності інформації [9].

Варіант класифікації показано на рис.1.1

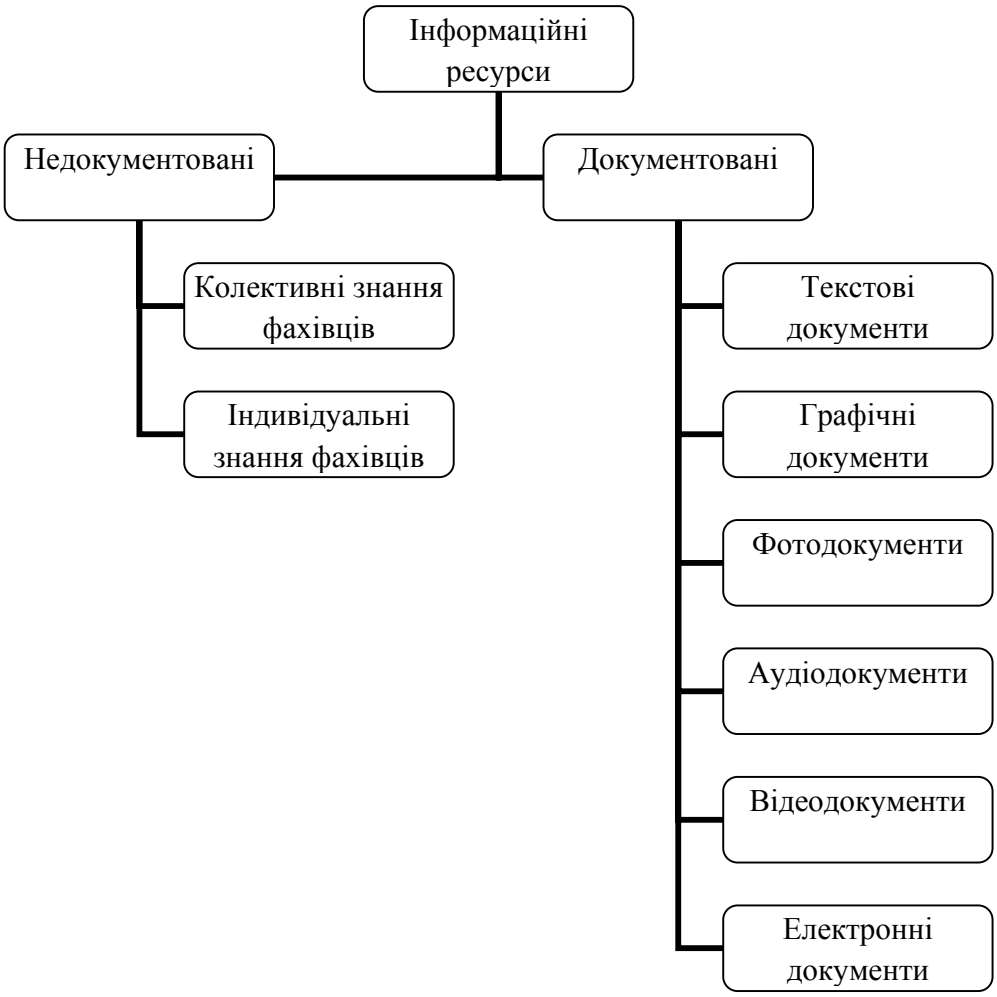

Рисунок 1.1 – Класифікація інформаційних ресурсів

«Національні інформаційні ресурси — це результати інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані на відповідних матеріальних носіях інформації як окремі документи і масиви документів, бази і банки даних та знань, усі види архівів, бібліотеки, музейні фонди тощо, які містять дані, відомості і знання, що є об’єктом права власності будь-якого суб’єкта України і мають споживчу цінність (політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо)» [10].

1.2 Електронні інформаційні ресурси

Стратегія воєнної безпеки України [11] передбачає серед іншого «адаптивне до змін безпекового середовища та збалансоване з можливостями держави використання людського капіталу, інформаційних, матеріальних, фінансових ресурсів України, їх підсилення ресурсами держав-партнерів» [12].

Адаптивне та збалансоване використання, вибір методів та засобів захисту залежать від виду та призначення ІР. Стрімкий розвиток інформаційних технологій зумовив важливе значення електронних інформаційних ресурсів. Тому актуальною є проблема визначення поняття «електронний інформаційний ресурс» та ознак класифікації ЕІР [12].

Поняття ЕІР визначається у правовому просторі, зокрема, Законом України «Про Національну програму інформатизації як «термін «електронні ресурси» вміщує такі аспекти поняття, як цифрова форма фіксації інформації, комп’ютерні засоби та програмне забезпечення для відтворення та керування, електронне середовище для розповсюдження (комп’ютерні мережі та засоби телекомунікаційного зв’язку).»» [13]. У наведеному визначенні в першу чергу вказується ідея цифрової форми фіксації інформації, що підкреслює заміну традиційних носіїв даних на цифрові формати, які можуть бути ефективно збережені та передаватися за допомогою електронних пристроїв. Для доступу до цифрових даних потрібні спеціальні технічні

засоби, які забезпечують оброблення та відображення цих даних для користувача. Визначення у Законі підкреслює значущість інформаційних технологій та інфраструктури зв'язку для ефективного поширення цифрової інформації в електронному форматі. Зазначене визначення EIP в правовому просторі України відображає ключові аспекти, пов'язані з цифровими даними, інформаційними технологіями та інфраструктурою зв'язку, які є необхідними для розуміння і реалізації сучасних інформаційних процесів у державі.

У понятті EIP відображено їх універсальну природу та сутність, що пролягає поза конкретним змістом, формою чи часом їх створення. Визначення включає ідею ресурсів, які призначені для вирішення різноманітних потреб громадян, суспільства та держави, виходячи з певних завдань, що стоять перед ними [2].

У контексті наведеного визначення, EIP виявляються важливим елементом для забезпечення доступу до необхідної інформації та вирішенням різноманітних суспільних потреб. Вони можуть включати в себе широкий спектр джерел, як державні, так і приватні, виходячи з різноманітних галузей діяльності та інформаційних потреб суспільства. Отже, таке визначення надає можливість розуміти EIP як важливий компонент інформаційного простору, спрямований на забезпечення потреб громадян, суспільства та держави в умовах сучасної цифрової епохи [2].

У табл.1.1 наведені визначення поняття «електронні інформаційні ресурси», які використовуються у нормативних документах України та роботах науковців [12].

У «Положенні про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» [14] зазначається, що «Державні електронні інформаційні ресурси — відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством». Це визначення вказує на важливість електронної інформації для держави та суспільства, підкреслює необхідність її захисту згідно з законодавством, яке визначає ступінь конфіденційності, цілісності та доступності інформації, встановлює обов’язки та відповідальність за її захист. Згідно з цим

документом, ІР мають бути зареєстровані і внесені до відповідного реєстру, що може бути важливим для контролю, моніторингу та керуванням цими ресурсами [14].

Таблиця 1.1 – Формулювання поняття ЕІР

№	Формулювання визначення ЕІР
1	ЕІР – систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних засобів та/або програмних продуктів.
2	ЕІР – інформація, апаратні, програмні та інші засоби, що можуть бути надані користувачеві, наприклад, файл-сервером або базою даних. На файл-сервері вся сукупність документів подана файлами, які зберігаються в пам’яті комп’ютера з певним кодовим позначенням. Змістом файлу може бути зміст документа або інша інформація, що стосується документа. В базах даних сукупність документів подана одним або кількома спеціально-організованими файлами.
3	ЕІР – інформаційні ресурси, що розміщені в електронних базах або банках даних, у комп’ютерних системах, системах автоматизованої обробки і передачі даних. При їх одержанні чи передачі за допомогою мережі Інтернет, їх називають веб-ресурсами.
4	ЕІР – вміщує такі аспекти поняття, як цифрова форма фіксації інформації, комп’ютерні засоби та програмне забезпечення для відтворення та керування, електронне середовище для розповсюдження (комп’ютерні мережі та засоби телекомунікаційного зв’язку).
5	ЕІР – інформаційні ресурси, якими управляє комп'ютер, у тому числі ті, що потребують використання периферійного пристрою, підключеного до комп'ютера.
6	ЕІР – інформаційний ресурс, який зберігається в електронному чи комп’ютеризованому форматі та може бути досягнутий, знайдений та перетворений засобами електронної мережі або іншої електронної технології обробки даних.

Національні ЕІР — ІР незалежно від їх змісту, форми, часу та місця створення, форми власності, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадянина, суспільства, держави. Національні ЕІР включають державні, комунальні та приватні ресурси [10].

У табл.1.2 [12] наведено визначення певних видів ЕІР, зокрема національних ЕІР, державних ЕІР, науково-освітніх ЕІР, освітніх ЕІР.

Таблиця 1.2 – Формулювання поняття ЕІР

№	Визначення деяких видів ЕІР
1	Національні ЕІР – інформаційні ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадянина, суспільства, держави. Національні електронні ресурси включають державні, комунальні та приватні ресурси.
2	Державні ЕІР – відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством.
3	Державні ЕІР – державні інформаційні ресурси незалежно від їх змісту, форми, часу і місця створення, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадян, суспільства, держави. Державні електронні інформаційних ресурсів є складовою Національного реєстру електронних інформаційних ресурсів.
4	Державні ЕІР – систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних та/або програмних засобів державних органів.
5	Державні ЕІР – систематизована, закріплена на матеріальних носіях і/або відображена в електронному вигляді інформація, право на володіння, використання або розпорядження якою належить державі або яка обробляється фізичними чи юридичними особами відповідно до наданих їм повноважень суб’єктами владних повноважень, призначена для задоволення потреб громадянина, суспільства, держави.
6	Науково-освітні ЕІР – електронні ресурси, які наповнюють науково-освітній інформаційний простір з метою цільового їх використання.
7	Освітні ЕІР – засоби навчання на цифрових носіях будь-якого типу або розміщені в інформаційно-телекомунікаційних системах, які відтворюються за допомогою електронних технічних засобів і застосовуються в освітньому процесі.
8	Бібліотечні ЕІР – опубліковані та неопубліковані первинні й вторинні документи на електронних носіях (книги, серійні видання, дисертації тощо), фактографічні, повнотекстові й бібліографічні бази даних.

EIP можна класифікувати за різними ознаками, приклади яких наведено у табл. 1.3.

Таблиця 1.3 – Класифікація електронних інформаційних ресурсів

Ознака	Приклад
За типом ресурсу	Електронні дані, програми, комбіновані: інтерактивні мультимедійні онлайн служби.
За технологією розповсюдження	Локальні електронні видання, мережні, комбінованого розповсюдження.
За характером взаємодії з користувачем	Детерміновані електронні інформаційні ресурси, недетерміновані ресурси.
За ступенем структурування	Від безперервного тексту, який не має розподілу на абзаци, параграфи тощо, до формального представлення інформаційних даних у базах даних.
За формою існування	База даних, вебсайт
За статусом	Оригінал, електронний аналог видання, електронна версія, електронний документ, електронний документ

Узагальнене визначення та класифікація EIP [12] на підставі різних ознак класифікації наведена на рис. 1.2.

Рисунок 1.2 – Визначення та класифікація EIP

2 СТРУКТУРА ІР ТА ЕІР ПІДПРИЄМСТВА

У сучасному економічному середовищі, яке визначається стрімкими змінами технологій та цифровою трансформацією, питання ефективного управління ІР стає ключовим для конкурентоспроможності та стійкості підприємств. ІР, включаючи ЕІР, представляють собою важливі активи, які допомагають забезпечити виробничі процеси, управління, маркетинг та стратегічне планування в організації. Підприємства в умовах інформаційного суспільства повинні бути готовими до використання сучасних інструментів та методів управління інформаційними ресурсами для досягнення успіху та забезпечення конкурентоспроможності.

Один із ключових аспектів в управлінні ІР підприємства полягає в розумінні структури цих ресурсів, яка передбачає не тільки їх фізичну організацію, а й методи, що використовуються для їх обробки, зберігання та передачі. До того ж, у зв'язку зі зростанням обсягів та складності інформації, значення ЕІР, які забезпечують зберігання та обробку даних у цифровій формі, стає важливішим у сучасному бізнес-середовищі. Вивчення структури та основних принципів управління ЕІР є невід'ємною частиною стратегії підприємства для забезпечення ефективного функціонування та досягнення стратегічних цілей.

У підприємств часто існують різні системи, які збирають інформацію різних типів. Ці системи часто зростають швидше, ніж вони можуть бути організовані, щоб задовольнити потреби бізнесу. Як результат, виникають відокремлені інформаційні ланцюги, які мають обмежений контакт один з одним. Однак багато з цих даних пов'язані між собою, і компанія, яка може об'єднати ці різні джерела даних, отримає значну перевагу.

ІР підприємства включають в себе набір нематеріальних активів та документів, які є важливими для стратегічного функціонування організації. Ці ресурси використовуються для підтримки виробничих процесів, прийняття управлінських рішень та забезпечення освіти.

ІР підприємства формуються з внутрішнього та зовнішнього середовища, що включає структурні підрозділи компанії та працівників, а також взаємовідносини між ними. Залежно від джерела виникнення інформації, вона може бути внутрішньою або зовнішньою, і сприймається як ресурс підприємства. Внутрішня інформація зазвичай є точною та відображає фінансовий стан компанії, і її обробка може здійснюватися за допомогою стандартних процедур. Ця інформація охоплює дані про працівників, продукцію, витрати, послуги, технологічні процеси, споживачів, канали збуту тощо.

Розглянемо підприємство, яке займається розробкою освітніх інструментів для українських та закордонних платформ. На цьому підприємстві використовуються стандартні документи, база даних клієнтів та працівників, правові документи та технічна документація (рис. 2.1).

Рисунок 2.1 – Структура ІР підприємства

2.1.Бази даних

У світі сучасних технологій бази даних використовуються у багатьох галузях, включаючи бізнес, освіту, науку, уряд та багато інших. Вони є невід'ємною частиною сучасних інформаційних систем і допомагають організаціям ефективно управляти інформацією для прийняття обґрунтованих рішень та оптимізації різноманітних процесів.

База даних (БД) – це впорядкована організована сукупність взаємозв’язаних даних, призначених для зберігання, накопичення та обробки інформації за допомогою електронно-обчислювальних машин [15]. Узагальнена схема роботи БД показана на рис. 2.2.

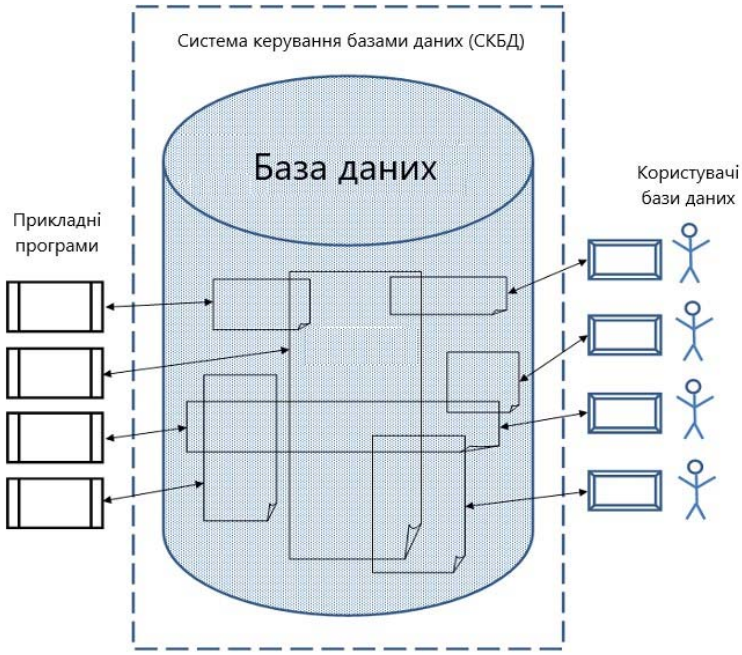

Рисунок 2.2 – Схема роботи БД

Зважаючи на визначення, слід зазначити що дані в БД організовані у вигляді структурованого набору, де вони взаємозв'язані та впорядковані таким чином, що дозволяє ефективно виконувати операції зберігання, оновлення та отримання даних.

Основною метою БД – є зберігання та впорядкування великого обсягу інформації. Користувачі мають можливість отримувати швидкий доступ та змінювати інформацію за потреби. Управління базами даних відбувається за допомогою спеціалізованого програмного забезпечення (СКБД), яке дозволяє створювати зберігати та модифікувати отримані дані.

Зв'язок між сучасним світом технологій і БД важко переоцінити. БД є основою функціонування багатьох сучасних програм і вебсайтів. Вони забезпечують ефективне зберігання, організацію та управління великим обсягом даних, що використовуються у різних галузях, включаючи бізнес, науку, освіту, технології, медицину та інші.

У сучасному світі існує багато популярних БД, кожна з яких має свої особливості і пристосована для конкретних сценаріїв використання. Ось кілька з них, які широко використовуються та є основою для багатьох сучасних додатків і систем:

MySQL: Це одна з найпопулярніших відкритих реляційних систем управління БД (СУБД). Вона широко використовується для зберігання даних в інтернет-додатках, таких як блоги, електронні магазини та форуми [16].

PostgreSQL: Ще одна популярна відкрита реляційна БД з багатьма додатковими можливостями, які роблять її популярною для підприємств і великих організацій. Вона володіє потужними можливостями розширення та додатковими функціями безпеки [16].

MongoDB: Ця БД використовує документо-орієнтовану модель даних і часто використовується для веб-розробки та інших сучасних додатків. MongoDB дозволяє швидший розвиток додатків шляхом швидкого зберігання та витягування даних [16].

Oracle Database: Це одна з найпотужніших та надійних реляційних СУБД, яка використовується в багатьох великих підприємствах для управління великим обсягом даних та даними високої важливості [16].

Microsoft SQL Server: Ця СУБД розроблена компанією Microsoft і широко використовується в кількох великих організаціях. Вона пропонує широкий набір інструментів для управління даними та дозволяє розробникам ефективно працювати з великими обсягами даних [16].

Redis: Ця БД відкритого коду використовується для зберігання даних в оперативній пам'яті і широко використовується для кешування даних та оптимізації продуктивності додатків [16].

БД використовуються для зберігання та організації даних, що дозволяє ефективне управління і доступ до інформації. Вони дозволяють зберігати великі обсяги даних у структурованому та систематизованому вигляді, що полегшує їхнє використання для аналітики, прийняття рішень, забезпечення безпеки та інших цілей. Крім того, БД дозволяють багатьом користувачам одночасно працювати з одними і тими ж даними, що сприяє спільній роботі та обміну інформацією.

Звертаючи увагу на специфіку нашого підприємства, слід зазначити що підприємство може мати БД для зберігання інформації про працівників, державних замовників та хронологію виконаних робіт.

У зазначеному підприємстві може використовуватися документо-орієнтована БД Mongo DB, яка надає гнучку структуру для зберігання даних у форматі BSON (Binary JavaScript Object Notation). БД може бути структурована: у колекції «Користувачі» для вміщення особистих даних користувачів, «Робітники» для інформації про працівників підприємства та «Проекти» для деталей освітніх ініціатив. Кожен документ у відповідній колекції містить релевантні атрибути, такі як ім’я, контактна інформація, посада, данні освітніх курсів та інші важливі IP [16].

У взаємодії з БД використовуються мови запитів Mongo DB, для отримання, оновлення та видалення даних. Агрегаційні функції використовуються для обчислення метрик, забезпечуючи необхідний аналітичний інструментарій. Кожен запит обчислюється за допомогою індексів, для поліпшення швидкодії операцій пошуку та фільтрації [16].

Забезпечення безпеки даних реалізується через вбудовані механізми аутентифікації та авторизації, а також шифрування даних для збереження конфіденційності інформації (протоколи Transport Layer Security, Secure Socket Layer) [16].

2.2 Технічна документація

Технічна документація (ТД) – це вимоги безпеки інформаційного середовища [17]. ТД з'являється в процесі документування різних видів науково-технічної діяльності, до яких належить проєктування, конструювання, розробка технологічних процесів, науково-дослідницька діяльність, організація промислового виробництва, а також геологорозвідувальні, геодезичні, картографічні роботи [17]. ТД має широкий спектр застосувань і включає в себе вимоги безпеки інформаційного середовища, що може стосуватися забезпечення конфіденційності, цілісності та доступності даних в системі. Крім того, ТД відображає всі необхідні дані, які виникають під час науково-технічної діяльності, такі як проєктування, конструювання, розробка технологічних процесів, науково-дослідна робота тощо. Це означає, що ТД є необхідним інструментом для збереження і передачі ключової інформації, пов'язаної з важливими технічними процесами та дослідженнями.

ТД має велике значення в будь-якій галузі, де потрібно забезпечити точність, надійність та безпеку при роботі з технічними даними. ТД допомагає уникнути помилок, забезпечує єдність процесів і полегшує обмін інформацією між спеціалістами з різних галузей. Також вона є ключовим елементом при впровадженні стандартів безпеки інформації, що є надзвичайно важливим в сучасному цифровому середовищі.

Для підприємства яке займається розробкою освітніх інструментів для українських та закордонних платформ, ТД може охоплювати широкий спектр документів, що описують деталі, архітектуру, конфігурації, інструкції з

використання, процедури, правила та інші аспекти, пов’язані з програмним забезпеченням, мережами, інфраструктурою та іншими аспектами діяльності підприємства. А саме:

1) Політика інформаційної безпеки. Визначаються загальні принципи, цілі та стратегії, які використовуються у підприємстві для забезпечення захисту конфіденційної інформації та інших внутрішніх ресурсів.
2) Стандарти безпеки. Надають комплексний підхід до управління інфраструктурою підприємства. Забезпечення аутентифікації та авторизації користувачів, контролю доступу до мережевого периметру, використання брандмауерів та інших систем безпеки. Впровадження систем виявлення вторгнень та систем запобігання вторгнень – є основними компонентами стандартів безпеки. Стандарти безпеки також визначають алгоритми шифрування, їх використання у конкретних сценаріях та управління ключами доступу. Специфікації алгоритмів, таких як асиметричне (RSA, ECC) або симетричне (TDEA, AES) шифрування, визначаються з урахуванням оптимальності та безпеки.
3) Процедури реагування на інциденти. Інструкції для робітників підприємства стосовно виявлення, діагностики та відновлення систем після інцидентів безпеки. Описують дії під час виявлення інциденту, класифікації інциденту (тип, потенційний вплив), повідомлення та сповіщення, аналіз інциденту, заходи з управління інцидентами.
4) Аудит безпеки. Процес тісно пов’язаний з визначенням обсягу та цілей аудиту безпеки, стандартів та вимог, процесом виконання аудиту, формуванням даних про технічні та організаційні аспекти безпеки, проведенням тестувань на проникнення, виявлення вразливостей та інших технічних перевірок.
5) Політика управління доступом. Визначення прав доступу користувачів до різних IP. Для більшості працівників підприємства доцільно використовувати

рівень доступу «користувач», в залежності від прав доступу більш значущі IP доступні лише за наявності рівня доступу «адміністратор».

ТД допомагає забезпечити якість продукту, покращити комунікацію між різними відділами підприємства, сприяє ефективному управлінню проєктами та забезпечує належне функціонування систем.

3 МЕТОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЙНОГО ЗАХИСТУ ЕІР

З поглибленням використання ЕІР у сучасному суспільстві постає все більш актуальне питання забезпечення їх надійності та безпеки. Захист цих ресурсів від несанкціонованого доступу, руйнування, втрати чи модифікації має вирішальне значення для збереження конфіденційності, цілісності та доступності інформації.
Діючими методами та засобами захисту ЕІР є:

Політика безпеки: розроблення комплексної політики безпеки, яка включає в себе правила користування, контроль доступу, шифрування даних, відповідальність співробітників тощо. Впровадження обов'язкового підписання всіма співробітниками угод щодо забезпечення конфіденційності та безпеки даних.

Фізична безпека: встановлення систем контролю доступу та відеоспостереження для обмеження фізичного доступу до серверних приміщень і обладнання. Захист обладнання від фізичних пошкоджень шляхом використання спеціальних корпусів, замків, систем тривоги тощо.

Кібербезпека: використання сучасних систем мережного брандмауеру та виявлення вторгнень для захисту від хакерських атак та зловживань. Постійне оновлення та моніторинг антивірусного програмного забезпечення для виявлення та нейтралізації шкідливих програм.

Шифрування даних: використання сучасних алгоритмів шифрування для захисту конфіденційної інформації під час трансляції та зберігання на серверах та в хмарних сервісах.

Аудит та моніторинг: постійний аудит безпеки для виявлення можливих вразливостей та вдосконалення систем безпеки. Встановлення систем моніторингу, які виявляють незвичайну активність та вчасно сповіщають про можливі атаки.

Резервне копіювання та відновлення даних: створення системи резервного копіювання для забезпечення безпечного зберігання даних та їх відновлення в разі випадкового видалення або пошкодження.

Культура безпеки: організація системи нагород та заохочень для стимулювання правильної культури безпеки серед співробітників. Забезпечення постійної освіти та тренінгів з питань кібербезпеки для всіх співробітників.

Важливе значення має реалізація засобів захисту програмного забезпечення підприємства (рис. 3.1).

Рисунок 3.1 – Засоби захисту ПЗ підприємства

3.1 Опис моделей загроз інформації та порушника

Один з кроків у створенні комплексної системи захисту інформації полягає у описі моделей загроз інформації та порушника. У описі моделі порушника доцільно розуміти класифікацію порушників, їх перелік, наслідки впливу.

Модель порушника – опис ймовірних дій порушника, рівня його повноважень, ресурсних можливостей, використовуваних ним програмних і (або) апаратних засобів з метою реалізації загроз для інформації [18]. Особу, яка хоче або може не санкціоновано отримати доступ до даних чи ресурсів у системі, слід вважати

порушником. При створенні моделі порушника важливо враховувати, що IP системи можуть бути привабливими для тих, хто прагне використовувати їх без дозволу. Ця привабливість зазвичай обумовлена типом та обсягом інформації, яка обробляється в системі. Якщо користувач намагається отримати несанкціонований доступ до об'єктів захисту, такий користувач вважається порушником [19].

Порушники, які можуть впливати на автоматизовану систему, поділяються на внутрішніх (власники, співробітники, користувачі системи) і зовнішніх (сторонні особи або ті, що не мають прямого доступу до системи). Модель порушника має визначати такі аспекти:

- категорії осіб, які можуть вчинити порушення;
- рівень доступу та можливостей, якими володіє порушник;
- припущення про рівень знань та кваліфікацію порушника;
- методи та способи, які використовуються для здійснення порушень;
- імовірна мета порушника та її вплив на систему;
- імовірне місця та способи для вчинення порушень;
- імовірні шляхи для здійснення загроз в автоматизованій системі;
- припущення щодо характеру дій, які порушник може вчинити.

Модель загроз – містить систематизовані дані про випадкові і навмисні загрози безпеці інформації. Систематизація даних моделі передбачає наявність відомостей про всі можливі загрози, їх небезпеку, часові рамки дії, вірогідність реалізації [2].

Для підприємства, що займається розробкою освітніх інструментів для українських та закордонних платформ, моделі загроз інформації та порушника можуть бути наступними:

1) Кібератаки: Можуть включати зловживання системи шляхом використання шкідливого програмного забезпечення, вірусів або зловмисних програм для злому системи та отримання неправомірного доступу до конфіденційної інформації.

2) Виток інформації: Може виникнути через недосконаліть внутрішньої політики безпеки, недостатні заходи контролю доступу або через недбаліть співробітників, що може призвести до втрати конфіденційної інформації.
3) Соціальний інжиніринг: Може включати маніпулювання людьми для отримання конфіденційної інформації шляхом обману, маніпулювання або шахрайства. Модель можливих загроз представлена у табл. 3.1.

Таблиця 3.1 – Модель можливих загроз

Назва загрози	Імовірність	Рівень шкоди	Метод реалізації
Кібератаки			
Віруси, троянські програми, фішингові атаки, DDoS-атаки	Середня	високий	Використання шкідливого програмного забезпечення для злому системи, отримання неправомірного доступу до конфіденційної інформації.
Виток інформації			
Недосконаліть внутрішньої політики безпеки, недостатні заходи контролю доступу, необережність співробітників.	Середня	високий	Витік даних через недостатньо захищені мережі, несанкціонований доступ до файлів або баз даних.
Соціальний інжиніринг			
Маніпулювання співробітниками для отримання конфіденційної інформації через обман або маніпуляцію.	середня	високий	Використання соціальних мереж, телефонних дзвінків, або електронної пошти для отримання довіри та конфіденційної інформації.

Модель порушника безпеки:

1) Внутрішній порушник: може бути працівник компанії, який намагається незаконно отримати доступ до конфіденційної інформації з метою особистої вигоди або злочинної діяльності.
2) Зовнішній порушник: може бути хакер, конкурент або інша сторона, що намагається зламати систему для отримання конфіденційної інформації з метою використання її власних цілей.
3) Колишній співробітник: може бути колишній працівник, який має знання про внутрішні системи та процеси компанії і може намагатися використати ці знання для шкоди підприємству.

Повноваження порушника:

- виконання певного набору програм або завдань;
- створення та використання власних програм або інструментів у системі;
- контроль за функціонуванням системи та можливість змінювати її конфігурацію;
- можливість підключення до апаратних засобів системи або внесення змін у їх конфігурацію.

Технічна оснащеність порушника:

- апаратні засоби;
- спеціальні засоби;
- програмні засоби.

Модель порушника представлена у табл. 3.2

Таблиця 3.2 – Модель порушника

Вид порушника	Повноваження порушника	Технічна оснащеність порушника
Внутрішній порушник		
Працівник компанії, що намагається незаконно отримати доступ до конфіденційної інформації для особистої вигоди або злочинної діяльності.	Виконання набору програм або завдань, створення та використання власних програм або інструментів у системі, контроль за функціонуванням системи та можливість змінювати її конфігурацію, підключення до апаратних засобів системи або внесення змін у їх конфігурацію.	Порушник може мати доступ до апаратних засобів, спеціальних засобів та програмного забезпечення.
Зовнішній порушник		
Хакер, конкурент або інша сторона, що намагається зламати систему для отримання конфіденційної інформації для своїх цілей.	Використання спеціальних програм або інструментів для незаконного доступу, контроль за деякими функціями системи, можливість впливати на роботу системи ззовні.	Володіння спеціальними програмами та знання про технічні вразливості системи.
Колишній співробітник		
Колишній співробітник зі знанням внутрішніх систем та процесів компанії, який може використовувати ці знання для шкоди.	Знання процесів та систем компанії, можливість впливати на внутрішні процеси і налаштування системи.	Знання про внутрішні робочі процеси, доступ до внутрішніх мереж і програмного забезпечення.

3.2 Електронні та електронні цифрові підписи

Електронний підпис (ЕП) — це електронні дані у зашифрованій формі, які додаються підписантом до інших електронних даних, наприклад електронних документів, звітності, або ж логічно з ними пов’язуються та використовуються ним як замінник справжнього особистого підпису [20]. Призначення ЕП – використання під час створення електронних документів, ст. 6 Закону «Про електронні документи та електронний документообіг» від 22.05.2003 № 851 [20]. Ключовим у використанні ЕП є Закон України «Про електронні довірчі послуги» [22].

ЕП поділяються на удосконалені та кваліфіковані. Удосконалений ЕП формується шляхом застосування криптографічних методів до електронних даних з використанням особистого ключа, що є унікально пов'язаним з особою, що його створює. Кваліфікований електронний підпис (КЕП) – це форма покращеного ЕП, створюється за допомогою системи КЕП та ґрунтується на спеціальному сертифікаті відкритого ключа [22].

Ключова різниця між ЕП та КЕП – рівень захисту та довіри до особистого ключа ЕП. У КЕП ключ розміщений на захищеному носії [22]. При перевірці ЕП обидва типи — удосконалений та кваліфікований, проходять перевірку. Проте, у випадку кваліфікованого ЕП, крім перевірки цілісності коду ЕП, також перевіряється, чи зберігається ключ на спеціальному кваліфікованому носії, наприклад, на флешці-токені. Якщо ключ знаходиться на іншому носії, що не є офіційним кваліфікованим засобом, система повинна повідомити, що немає підтвердження того, що особистий ключ знаходиться на кваліфікованому засобі ЕП. Пристрій-носій КЕП має відповідати п. 2 Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженому постановою Кабміну від 19.09.2018 № 749 [23].

Згідно із Законом України «Про електронні довірчі послуги» [22], КЕП чи печатка вважаються підтвердженими, якщо під час перевірки за допомогою кваліфікованого сертифіката ЕП чи печатки було підтверджено, що особистий ключ, який використовується, знаходиться відповідно на кваліфікованому носії.

Засоби КЕП чи печатки мають забезпечувати захист від доступу до особистих ключів сторонніх осіб згідно з вимогами Закону. Пункт 12 статті встановлює, що кваліфіковані сертифікати відкритих ключів повинні містити відомості про розташування особистого ключа на кваліфікованому носії.

У сфері захисту інформації офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України [24] розмістив роз'яснення стосовно використання засобів ЕП та печатки для надання кваліфікованих електронних довірчих послуг. Таким чином, використання КЕП передбачає, що особистий ключ повинен бути збережений відповідно на кваліфікованому носії та пов'язаний з кваліфікованим сертифікатом ЕП.

Також слід враховувати, що відповідно до постанови Кабінету Міністрів України від 03.03.2020 N 193, можна використовувати удосконалені ЕП чи печатки на основі кваліфікованих сертифікатів відкритих ключів для електронної взаємодії, ідентифікації та автентифікації, якщо Закон передбачає використання КЕП чи печаток, крім випадків, що передбачені законодавством [25].

Необхідно зазначити, що кваліфікований сертифікат відкритого ключа для удосконаленого ЕП чи печатки не містить інформації про розташування особистого ключа на кваліфікованому носії, і під час перевірки удосконаленого підпису чи печатки за допомогою кваліфікованого сертифіката відкритого ключа надається підтвердження, що особистий ключ не знаходиться на кваліфікованому носії.

Електронний цифровий підпис (ЕЦП) – це дані в електронній формі, отримані за результатами криптографічного перетворення, які додаються до інших даних або документів і забезпечують їх цілісність та ідентифікацію автора [24]. ЕЦП використовується для підписання електронних документів та доступу до онлайн-

послуг, в тому числі на державних порталах. Ця технологія є еквівалентом звичайного паперового підпису з юридичної точки зору. Відповідно, документи, що підписані за допомогою ЕЦП, мають повну юридичну силу, так само, як і традиційні паперові документи.

У середині 2018 року близько 9 мільйонів фізичних осіб та представників юридичних осіб уже користувалися ЕЦП. З цієї кількості, приблизно третина складалася з фізичних осіб, фізичних осіб-підприємців та самозайнятих осіб.

Слід зазначити, що назва «Електронний цифровий підпис» є застарілою, оскільки з’явилася у 2018 році. Однак, те що називають ЕЦП, згідно Закону «Про електронні довірчі послуги» [22], можна вважати удосконаленим ЕП.

У сучасному цифровому світі, де електронні документи та транзакції стають все більш поширеними, виникає необхідність у забезпеченні їхньої автентичності та недоторканості. Два ключових засоби для цього – ЕЦП та традиційний власноручний підпис. Ці дві форми підпису мають суттєві відмінності, які потрібно розглянути для забезпечення надійності та юридичної сили документів.

Доцільно порівняти їх за такими критеріями, як юридична сила, процес створення, зручність використання та застосування у сучасному бізнес середовищі (табл. 3.3).

Отже, ЕП та власноручний підпис відрізняються за своїми основними характеристиками та вимогами. ЕП є змінним і залежить від тексту, вимагає підготовки складної інфраструктури сертифікатів ключів та використовує додаткові механізми для виконання алгоритмів підпису та перевірки. З іншого боку, власноручний підпис завжди залишається однаковим незалежно від тексту, не має залежностей від допоміжних інструментів та не потребує підтримувальної інфраструктури. Обидва види підпису мають свої переваги та обмеження, які потрібно враховувати при їхньому використанні в різних сферах та контекстах.

Таблиця 3.3 – Порівняння ЕП та власноручного підпису

Електронний підпис	Власноручний підпис
Залежить від тексту, є змінним	Завжди однаковий, не має залежності від тексту
Особа, яка підписує документ, може мати декілька конфіденційних ключів, однак передача їх третім особам заборонена. ЕП може бути складним (у випадку удосконаленого ЕП) або дуже складним (у випадку КЕП) для підробки. При цьому існує ризик його втрати.	Має тісний зв’язок з особою, яка його створює, і зазвичай використовується лише один вид підпису. Неможливо передати його іншим людям, але можливо підробити. Загубити його також неможливо.
Дійсний для всіх копій документа	Має зв’язок безпосередньо з документом і вимагає окремого підпису для кожної його копії.
Для виконання алгоритмів підпису та перевірки необхідно використовувати додаткові методики та процедури.	Не має залежностей від допоміжних інструментів.
Потребує підготовки складної інфраструктури сертифікатів ключів.	Не потрібна підтримувальна інфраструктура.

У контексті підприємства, яке займається розробкою освітніх програм для українських (державних) та закордонних замовників, використання ЕП має величезну кількість переваг:

- Забезпечення безпеки даних: ЕП гарантують цілісність та автентичність документів, забезпечуючи надійний захист від несанкціонованого доступу та змін. Це можуть бути як документи підприємства, так і документація яка використовується під час проходження Національного мультипредметного тесту, підписання студентами угод дистанційно, тощо.

- Ефективність та швидкість: використання ЕП дозволяє швидше здійснювати процеси підпису та обміну документами, що прискорює внутрішні та зовнішні операції підприємства, освітньої установи, онлайн школи.
- Масштабованість та легкість управління: ЕП дозволяють керувати багатьма документами та підписами одночасно, що спрощує масштабування бізнесу та його документаційний процес, податкову звітність.
- Екологічна ефективність: використання ЕП дозволяє уникнути великого обсягу паперової документації, сприяючи екологічно відповідним практикам.
- Відповідність нормативним вимогам: використання ЕП допомагає відповідати вимогам щодо цифрової підпису та документообігу, зокрема у сфері освіти та інформаційних технологій.

Ці переваги підтримують ефективну та безпечну розробку та обмін освітніми продуктами в рамках компанії, сприяючи підвищенню продуктивності та забезпеченню високої якості продукції.

Використання ЕП в Україні стає все більш поширеним і важливим для спрощення та урегулювання юридичних процесів. Застосування цієї технології допомагає зменшити бюрократичні бар'єри і зробити бізнес-процеси більш ефективними.

3.3 Верифікація облікових даних

Не менш важливим у забезпеченні інформаційної безпеки продуктів та працівників підприємства є використання підходу з Verifiable credentials (VC).

У наш час, замість того, щоб мати фізичні копії важливих документів, таких як паспорти, водійські права чи права власності на автомобіль, ми все частіше використовуємо їх цифрові версії. Ці цифрові дані мають унікальні криптографічні властивості, які забезпечують їхню надійність та захищеність від підробок. Вони

можуть бути використані тільки власником та підтверджені довіреними органами, що робить їх особливо безпечними для електронної взаємодії.

Ці нові можливості цифрових облікових даних принесли значні переваги усім сторонам. Для користувачів це спрощує взаємодію з онлайн-сервісами, надаючи надійний цифровий ідентифікаційний засіб. Уряди мають шанс на економічний розвиток через підвищення довіри в інтернет-послуги. Для підприємств це означає автоматизацію процесів, підвищення рівня довіри й ефективності, а також зниження шахрайства. Ці переваги підтверджують значення цифрових облікових даних як важливої складової у сфері самостійної ідентифікації.

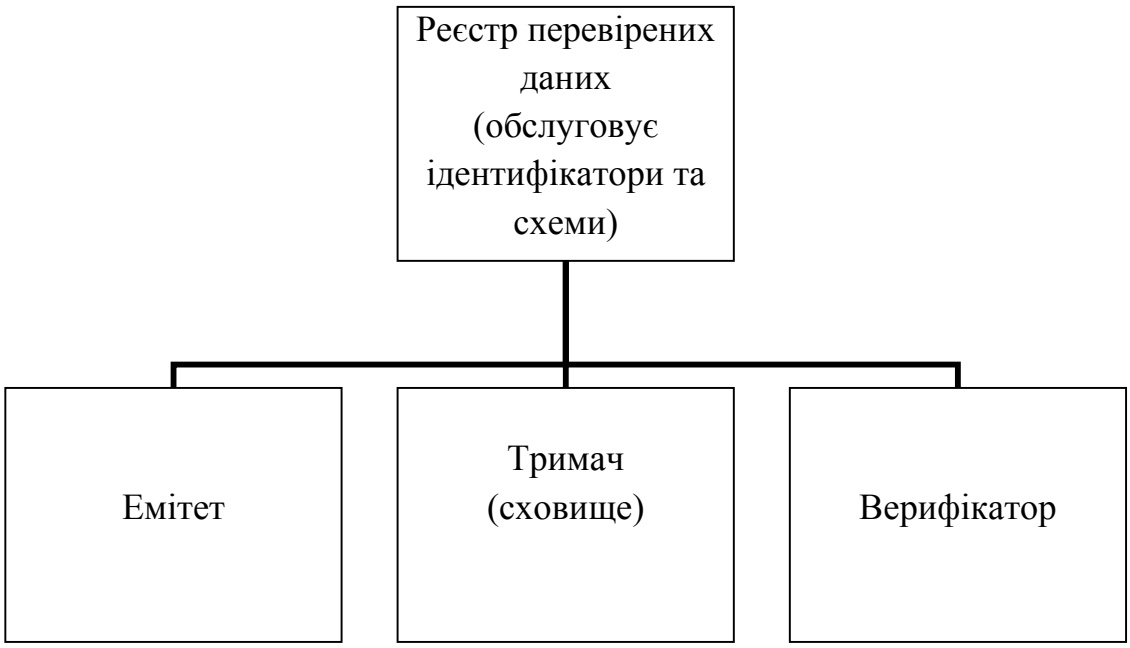

Рисунок 3.2 – Модель верифікації облікових даних W3C

На рис. 3.2 показана модель верифікації облікових даних: емітети створюють облікові дані, власники зберігають їх, а верифікатори запитують підтвердження на їх основі. Верифіковані презентації — це пакети доказів — або облікові дані, або дані, отримані з одного чи кількох облікових даних, — створені власниками, щоб

задовольнити вимоги верифікатора [26]. Верифікатори з упевненістю дізнаються, які емітети щось засвідчили, перевіряючи цифрові підписи з реєстром даних, який можна перевірити. З перевіреними претензіями верифікатор більше не повинен зв'язуватися з емітетом для підтвердження облікових даних. Це може заощаджувати сотні мільярдів щороку на витратах на перевірку даних галузям, які потребують адміністрування, як-от охорона здоров'я та страхування [27].

Верифікатори залишають за собою право визначати, чи є емітет надійним чи ні. Власник зберігає контроль і право власності на свою особистість. Власники вибирають, що вони хочуть розкрити, і кому вони хочуть це розкрити. Вони можуть ділитися лише необхідною інформацією і нічим більше [26]. Наприклад, вони можуть довести, що вони є зареєстрованими на освітній курс, або отримали сертифікат щодо проходження освітньої програми, не повідомляючи його ідентифікаційного номера.

VC у контексті підприємства, яке займається розробкою освітніх програмам допомагає покращити:

- Гнучкість та адаптивність: VC дозволяють студентам отримувати індивідуалізовані облікові дані, які відповідають їх конкретним освітнім потребам та досягненням.
- Безпека та захист даних: цей підхід дозволяє забезпечити безпеку та захист облікових даних студентів, у тому числі персональних досягнень та сертифікатів, за допомогою криптографічних методів.
- Легше відстеження прогресу: VC можуть служити як засіб відстеження освітнього прогресу студентів, що сприяє зручності для педагогічного персоналу та керівництва освітнього закладу.
- Підвищення конкурентоспроможності: застосування VC дозволяє компанії надавати студентам інноваційні та високотехнологічні засоби отримання освіти, що підвищує її конкурентоспроможність на ринку освітніх послуг.

- Покращений ефективний контроль ідентифікації: змінні облікові дані дозволяють зберігати інформацію про освітні досягнення студентів у форматі, що може бути легко ідентифікованим та перевіреним з точністю.

Всі ці переваги допомагають забезпечити ефективну та інноваційну освітню платформу для студентів, забезпечуючи їм гнучкий та безпечний шлях отримання якісної освіти та сертифікації.

3.4 Політика безпеки інформації

У сучасному цифровому світі, де інформація виступає як ключовий ресурс, забезпечення її безпеки стає однією з найважливіших пріоритетних завдань для організацій та підприємств усіх рівнів. Політика інформаційної безпеки визначає набір стратегічних заходів та рекомендацій, спрямованих на забезпечення захищеності електронних даних та ефективного управління ризиками їхнього неправомірного використання. Доцільним є розгляд аспектів політики безпеки інформації, її складових та важливості для сучасних організаційних процесів.

Важливо розуміти основні принципи та правила, що лежать в основі розробки ефективної політики безпеки інформації, стратегії запобігання несанкціонованому доступу до даних та впливу можливих загроз на їх конфіденційність та цілісність, важливість регламентації процедур та встановлення обмежень для забезпечення безпеки електронних даних, рекомендації щодо мінімізації ризиків інформаційного впливу на діяльність організацій.

Ефективна реалізація політики інформаційної безпеки є критично важливими для забезпечення стійкості та надійності функціонування сучасних підприємств у цифровому середовищі.

Політика інформаційної безпеки – це набір вимог, правил, обмежень та рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації [28].

Політику безпеки інформації реалізує служба захисту інформації (СЗІ), структура та завдання якої наведено у табл. 3.4.

Таблиця 3.4 – Структура та завдання служби захисту інформації

Напрямок	Обов'язки
Директор з інформаційної безпеки	- визначення стратегічних напрямків захисту інформації; - координація роботи служби захисту інформації з іншими підрозділами підприємства; - розробка політики інформаційної безпеки.
Відділ технічного захисту	- встановлення технічних засобів захисту інформації; - моніторинг та аналіз інформаційних загроз та інцидентів; - розробка та впровадження криптографічних засобів захисту.
Відділ адміністративного захисту	- розробка та впровадження правил користування інформацією на підприємстві; - навчання персоналу з питань безпеки інформації; - ведення контролю доступу до конфіденційної інформації.
Відділ аудиту та контролю	- проведення аудиту систем захисту інформації; - визначення вразливостей та розробка заходів щодо їх усунення; - встановлення процедур контролю за виконанням вимог політики інформаційної безпеки.
Відділ реагування на інциденти	- миттєва реакція на інформаційні загрози та інциденти; - відновлення роботи системи після кібератаки або інших подій; - аналіз причин виникнення інцидентів та вдосконалення заходів захисту.

Політика безпеки інформації визначає основні принципи, правила та процедури, які спрямовані на захист електронної інформації та забезпечення безпеки даних у підприємстві. Основна мета політики безпеки інформації полягає в забезпеченні конфіденційності, цілісності та доступності даних, запобіганні несанкціонованому доступу до інформації та мінімізації можливих загроз безпеці.

Основні складові політики безпеки інформації для підприємства, що займається розробкою освітніх інструментів, можуть включати:

- Класифікація даних: визначення різних рівнів конфіденційності для інформації і встановлення правил доступу до різних категорій даних.
- Правила використання інформації: встановлення чітких правил та процедур щодо збору, зберігання, обробки та обміну інформацією в межах підприємства.
- Управління доступом: регулювання прав доступу співробітників до різних типів даних відповідно до їхніх обов'язків та ролей у підприємстві.
- Заходи безпеки мережі: встановлення стандартів безпеки для захисту мережної інфраструктури від зовнішніх загроз та зловживань.
- Політика паролів: встановлення правил щодо створення та використання складних паролів для доступу до систем та додатків.
- Захист від зовнішніх загроз: використання антивірусного програмного забезпечення, брандмауерів та інших інструментів для захисту від зловмисних програм та кібератак.
- Навчання та свідомість: організація регулярних тренінгів та семінарів для співробітників з питань кібербезпеки та правил користування інформацією.
- Аудит та моніторинг: проведення систематичних аудитів та моніторингу для виявлення можливих вразливостей та ризиків для безпеки інформації.

Складові Політики безпеки інформації на підприємстві показано на рис. 3.7.

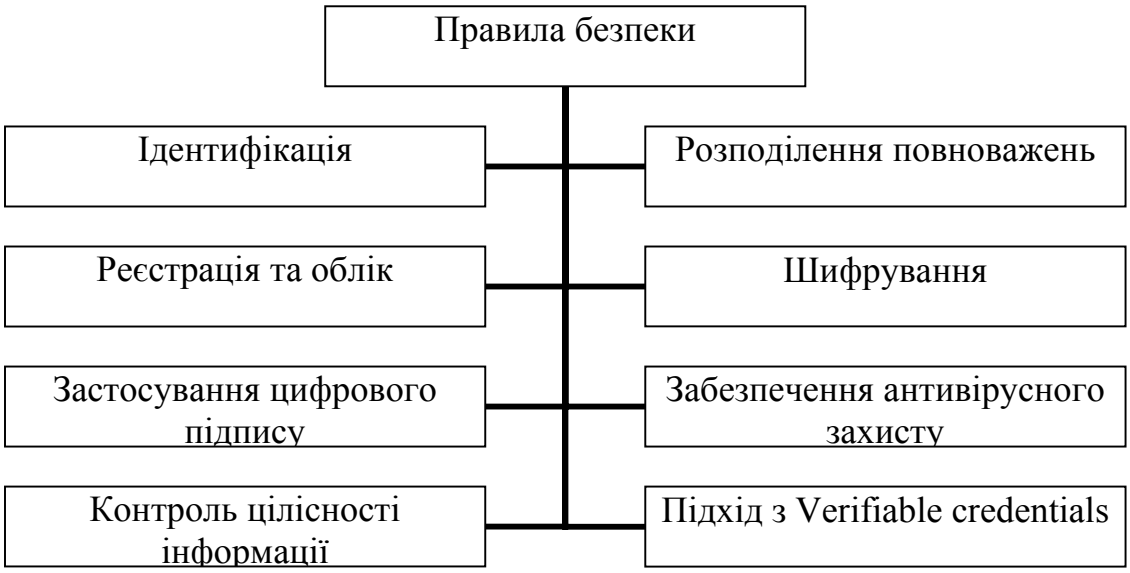

Рисунок 3.3 – Політика безпеки інформації

ВИСНОВКИ

У сучасному науковому та суспільному просторі поняття «інформаційні ресурси» набуло особливої значущості, оскільки вони стали ключовим елементом вирішення завдань, набуття знань та взаємодії з іншими системами. ІР можуть бути представлені як окремі документи, такі як текстові файли, таблиці, презентації, або як більш об'ємні масиви документів, які зберігаються в різних інформаційних системах. ІР є важливою складовою сучасного суспільства, їх правовий режим потребує уваги та розробки відповідних норм, а їх управління та захист є критичними завданнями для забезпечення безпеки та ефективного використання інформації.

У роботі були розглянуті різні типи ІР, зокрема, ІР спільного користування, які об'єднують державні органи, науково-технічні бібліотеки, комерційні центри тощо, а також ІР науково-технічної інформації, які включають науково-технічну літературу та документацію. Ключовим є необхідність ретельного захисту конфіденційної інформації для підприємств, а також визначень ключових понять та типів ІР, що використовуються в контексті наукових досліджень та практичної діяльності організацій.

Задля розуміння різноманітності ІР була розглянута їх класифікація, що базується на різних ознаках, таких як вид інформації, вид носія, режим доступу, спосіб організації зберігання та використання, спосіб формування та розповсюдження, а також форма власності.

У розділі про електронні інформаційні ресурси (ЕІР) було детально розглянуто поняття та ознаки класифікації ЕІР. Акцент був зроблений на значущості та ролі ЕІР у сучасному інформаційному просторі, а також їх важливості для різних сфер життєдіяльності. ЕІР відображають універсальну природу та сутність, яка пролягає поза конкретним змістом, формою чи часом їх створення. Вони використовуються

для вирішення різноманітних потреб громадян, суспільства та держави, виходячи з певних завдань, що стоять перед ними.

Управління ІР є ключовим елементом для забезпечення ефективного функціонування підприємств у сучасному економічному середовищі. ІР, включаючи електронні, відіграють важливу роль у підтримці виробничих процесів, управління, маркетингу та стратегічного планування. Розуміння структури ІР підприємства є важливим для ефективного управління цими ресурсами. В умовах зростання обсягів і складності інформації важливим стає розуміння та ефективне управління EIP. Ці ресурси допомагають забезпечити зберігання та обробку даних у цифровій формі, що впливає на конкурентоспроможність підприємства. Важливість об'єднання різних джерел даних в межах підприємства підкреслюється, оскільки це дозволяє отримати значну конкурентну перевагу. Управління великим обсягом інформації і його зв'язків є важливим елементом для забезпечення ефективного функціонування підприємства.

У роботі були розглянуті бази даних (БД), оскільки вони є невід'ємною частиною сучасних інформаційних систем у багатьох сферах, включаючи бізнес, науку, освіту та уряд. У контексті підприємства БД використовуються для зберігання інформації про працівників, державних замовників та хронологію виконаних робіт. БД дозволяють ефективно керувати великим обсягом даних, полегшуючи їхнє використання для аналітики, прийняття рішень, забезпечення безпеки та спільної роботи користувачів.

Так само як і бази даних, технічна документація (ТД) має велике значення в будь-якій галузі, де важлива точність, надійність та безпека при роботі з технічними даними. Вона сприяє уникненню помилок, єдності процесів та полегшує обмін інформацією між спеціалістами з різних галузей. Для підприємства, яке займається розробкою освітніх інструментів, ТД охоплює широкий спектр документів, пов'язаних з програмним забезпеченням, мережами, інфраструктурою та іншими аспектами діяльності підприємства. ТД допомагає забезпечити якість продукту,

поліпшує комунікацію між різними відділами підприємства, сприяє ефективному управлінню проектами та забезпечує належне функціонування систем.

У роботі був наведений опис ймовірних дій порушника, рівня його повноважень, ресурсних можливостей, використовуваних програмних і (або) апаратних засобів з метою реалізації загроз для інформації. Для підприємства, що займається розробкою освітніх інструментів, моделі загроз та порушника включають кібератаки, виток інформації та соціальний інжиніринг. Ці моделі допомагають розуміти потенційні загрози та забезпечити належний рівень безпеки інформації. Аналіз імовірних дій порушника є важливим задля розуміння потенційних загроз безпеці інформації з боку різних типів порушників. Врахування цих моделей допомагає підприємству виявляти та запобігати можливим атакам, забезпечуючи відповідний рівень захисту та безпеки інформації.

Організаційні методи захисту, такі як політика безпеки, фізична безпека, кібербезпека, шифрування даних, аудит та моніторинг, резервне копіювання та відновлення даних, а також культура безпеки, є важливими компонентами ефективної системи безпеки інформації. Впровадження передових технологій, систем контролю та моніторингу, а також регулярне навчання та свідомість серед співробітників допомагають забезпечити високий рівень захищеності інформації в організації.

Не менш важливим для захисту інформації є електронний підпис (ЕП) та кваліфікований електронний підпис (КЕП). Ці інструменти є важливими для забезпечення цілісності та автентичності електронних документів у цифровому середовищі. Ключова різниця між ЕП та КЕП полягає в наявності спеціального кваліфікованого носія для особистого ключа в останньому, що дозволяє забезпечити вищий рівень безпеки. Використання ЕП та КЕП стає все більш поширеним у різних сферах діяльності, включаючи бізнес-середовище та органи державної влади. Необхідно уважно враховувати вимоги та нормативні акти, що регулюють використання електронних підписів, для забезпечення відповідності дій з вимогами

законодавства. Використання ЕП забезпечує безпеку даних, ефективність та швидкість обміну документами, масштабованість та легке управління, екологічну ефективність та відповідність нормативним вимогам. Впровадження ЕП сприяє спрощенню та урегулюванню юридичних процесів, зменшенню бюрократичних бар'єрів та підвищенню ефективності бізнес-процесів.

У роботі був розглянутий підхід з використанням Verifiable credentials (VC), який дозволяє забезпечити гнучкість, безпеку та ефективний контроль ідентифікації. Цифрові версії важливих документів мають унікальні криптографічні властивості, які забезпечують їхню надійність та захищеність від підробок. Підхід з використанням VC сприяє підвищенню конкурентоспроможності, покращенню ефективного контролю ідентифікації, легшому відстеженню прогресу студентів та забезпеченню індивідуалізованих облікових даних.

У останньому розділі роботи була розглянута політика безпеки інформації. Політика безпеки інформації визначає основні принципи, правила та процедури, які спрямовані на захист електронної інформації та забезпечення безпеки даних у підприємстві. Для підприємства, що займається розробкою освітніх інструментів, політика безпеки інформації має включати класифікацію даних, правила використання інформації, управління доступом, заходи безпеки мережі, політику паролів, захист від зовнішніх загроз, навчання та свідомість, аудит та моніторинг. Ці складові політики спрямовані на забезпечення конфіденційності, цілісності та доступності даних, запобігання несанкціонованому доступу до інформації та мінімізації можливих загроз безпеці.

За підсумками роботи отримані нові наукові результати, які знайшли відображення у наукових публікаціях, зокрема, у матеріалах 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті» (10-12 травня 2023 р.) та статті у Всеукраїнському науково-технічному збірнику «Радіотехніка» [12].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Комплексні системи захисту інформації / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – 2018. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil1.html (дата звернення 01.10.2023).

2. Конспект лекцій з дисципліни «Захист інформаційних ресурсів обмеженого доступу» для студентів спеціальності 125 «Кібербезпека», які навчаються за спеціалізацією «Системи технічного захисту інформації, автоматизація її обробки» / Упоряд.: І. О. Милютченко. − Харків: ХНУРЕ, 2017. − 245 с.

3. Інформаційні ресурси: аналіз категорії та класифікація / І.О. Милютченко, Б.В. Онопко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2018. Вип. 192. С. 157 - 161.

4. Про науково-технічну інформацію: Закон України від 19.04.2014 р. №3322-12. URL: zakon.rada.gov.ua/laws/show/3322-12 (дата звернення 01.10.2023).

5. Заплотинський Б. А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ «ОЮА», кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

6. Низенко Е. І., Каленяк В. П. Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — Київ : МАУП, 2006. — 134 с. — Бібліогр.: С. 124–130.

7. Загальні положення про інформаційні ресурси. URL: https://moodle.znu.edu.ua/pluginfile.php?file=/721431/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%203%20%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96%20%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%B8.pdf (дата звернення 01.10.2023).

8. Про національну програму інформатизації: Закон України від 16.10.2020 р. №74/98-ВР. URL: zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (дата звернення 01.10.2023).

9. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV-ВР//ВВР. — 2006. — № 30. — С. 258.

10. Юдін О. К. Правові аспекти формування системи державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Безпека інформації. — 2014. — Т. 20 (1). — С. 76–82. — Режим доступу: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/6578. (Журнал індексується у наукометричних базах даних)

11. Указ Президента України: Про Рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» від 25.03.2021 р. №121/2021 (дата звернення 01.10.2023).

12. Електронні інформаційні ресурси: визначення та класифікація / І.О. Милютченко, П.О. Кулько // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 65 - 69.

13. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 27-28. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80# (дата звернення 01.10.2023).

14. Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління : затверджено Постановою Кабінету Міністрів України від 3 серпня 2005 р. № 688 (у редакції від 07.09.2011 р. № 938). — Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/KP050688.html.

15. Маслянко П. П., Ліссов П. М. Інформаційні ресурси та підходи до вимірювання інформації // Вісник КУЕІТУ «Нові технології» – 2008, №2(20) – С. 300-307.

16. Рейтинг популярних баз даних у 2023 році. URL: db-engines.com/en/ranking (дата звернення 01.10.2023).

17. Технічна документація: методичні вказівки до вивчення курсу для студентів спеціальностей 7.02010501, 8.02010501 «Документознавство та інформаційна діяльність». – Кіровоград: КНТУ, 2015 – 52 с.

18. Технічний захист інформації на програмно-керованих АТС загального користування. – ДСТСЗІ СБ України – Київ, 28 с.

19. Методика оцінки загроз для інформації автоматизованих систем. М. Будько – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 10 вип. 2005 р.

20. Електронний підпис: види та використання. URL: https://buhplatforma.com.ua/article/7502-elektronniy-tsifroviy-pdpis#ancex0 (дата звернення 01.10.2023).

21. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. URL: zakon3.rada.gov.ua/laws/show/851-15 (дата звернення 01.10.2023).

22. Про електронні довірчі послуги: Закон України від 05.10.2027 р. № 2155-19. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення 01.10.2023).

23. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності: Постанова КМУ від 19 вересня 2018 року, №749. URL: https://zakon.rada.gov.ua/laws/show/749-2018-%D0%BF (дата звернення 01.10.2023).

24. Портал Державної служби спеціального зв’язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення 01.10.2023).

25. Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів: Постанова КМУ від 3 березня 2020 р. №193. URL: https://zakon.rada.gov.ua/laws/show/193-2020-%D0%BF (дата звернення 01.10.2023).

26. Verifiable Credentials Data Model v1.1 URL: https://www.w3.org/TR/vc-data-model (дата звернення 01.10.2023).

27. Verifiable Credentials URL: https://edx-credentials.readthedocs.io/en/latest/verifiable_credentials/overview.html (дата звернення 01.10.2023).

28. Інформаційна безпека. Чи працює Політика ІБ у Вашій компанії?. URL: https://legalitgroup.com/informaciyna-bezpeka-v-kompanii (дата звернення 01.10.2023).