Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

# МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**"Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону"**

Виконав: ст. 2-го курсу, групи 1КІТС-22м,
спеціальності 125 – Кібербезпека,
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)

Білоус В. М.
(прізвище та ініціали)

Керівник: д.т.н., проф., професор каф.МБІС

Яремчук Ю. Є.
(прізвище та ініціали)

«04» грудня 2023 р.

Опонент: к.т.н., доц., доцент каф. ОТ

Колесник І. С.
(прізвище та ініціали)

«04» грудня 2023 р.

**Допущено до захисту**
Голова секції УБ кафедри МБІС

Юрій ЯРЕМЧУК
“04” грудня 2023 р.

Вінниця ВНТУ – 2023 рік

Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти – ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма – Кібербезпека інформаційних технологій та систем

**ЗАТВЕРДЖУЮ**
**Голова секції УБ кафедри МБІС**
_____ **Юрій ЯРЕМЧУК**
“20” вересня 2023 р.

**З А В Д А Н Н Я**
**на магістерську кваліфікаційну роботу студенту**
Білоус Віталій Михайлович
(прізвище, ім`я, по-батькові)

1. Тема роботи:
«Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону»

Керівник роботи: д.т.н., проф. каф. МБІС МБІС Яремчук Ю.Є.
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “18” вересня 2023 року № 247.

2. Строк подання студентом роботи за тиждень до захисту.

3. Вихідні дані до роботи:
Стандарти, електронні джерела, підручники та наукові статті по темі, які стосуються теми магістерської кваліфікаційної роботи.

4. Зміст текстової частини:
Для досягнення мети роботи було поставлено такі задачі: проаналізувати основні засади забезпечення безпеки об’єктів критичної інфраструктури та, зокрема, її складової – інформаційно-телекомунікаційної інфраструктури; дослідити методи системного аналізу безпеки об’єктів, а також сучасні методи автентифікації користувачів інформаційного ресурсу; розробити базу даних консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури, виконати декомпозицію та отримати кінцеві відношення за методом нормалізації відношень; забезпечити захист створеного консолідованого інформаційного ресурсу; здійснити програмну реалізацію захищеного консолідованого інформаційного ресурсу та програмних модулів забезпечення захисту інформаційного ресурсу; здійснити системний аналіз безпеки інформаційно-телекомунікаційної інфраструктури регіону на основі реалізованих програмних засобів.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень)
У першому розділі магістерської кваліфікаційної роботи наведено 2 рисунки, у другому розділі – 7 рисунків, у третьому розділі – 18 рисунків.

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Основна частина | | | |
| I | Яремчук Ю.Є. д.т.н., проф. каф.МБІС | | |
| II | Яремчук Ю.Є. д.т.н., проф. каф.МБІС | | |
| III | Яремчук Ю.Є. д.т.н., проф. каф.МБІС | | |
| Економічна частина | | | |
| IV | Причепа І.В., к.е.н., доц. каф. ЕПВМ | | |

7. Дата видачі завдання 20 вересня 2023 р.

## КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів магістерської кваліфікаційної роботи | Строк виконання етапів роботи | | Примітка |
|---|---|---|---|---|
| 1. | Визначення напрямку магістерської роботи, формулювання теми | 20.09.2023 | 31.09.2023 | |
| 2. | Аналіз предметної області обраної теми | 01.10.2023 | 15.10.2023 | |
| 3. | Розробка роботи | 16.10.2023 | 26.10.2023 | |
| 4. | Написання магістерської роботи на основі розробленої теми | 27.10.2023 | 15.11.2023 | |
| 5. | Передзахист магістерської кваліфікаційної роботи | 16.11.2023 | 24.11.2023 | |
| 6. | Виправлення, уточнення, корегування магістерської кваліфікаційної роботи | 27.11.2023 | 04.12.2023 | |
| 7. | Захист магістерської кваліфікаційної роботи | 11.12.2023 | 17.12.2023 | |

**Студент** _____ Білоус В.М.
( підпис )

**Керівник роботи** _____ Яремчук Ю.Є.
( підпис )

# АНОТАЦІЯ


УДК 004.56.5(043.2)

Білоус В.М.. Розробка захищеного консолідованого інформаційного ресурсу системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону. Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем». Вінниця: ВНТУ, 2023. 135 с.

На укр.мові. Бібліогр.: 63 назв; рис.: 16; табл. 13.

Метою магістерської роботи є розробка захищеного консолідованого інформаційного ресурсу системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону.

З’ясовані особливості безпеки об’єктів критичної інфраструктури загалом і інформаційно-телекомунікаційної інфраструктури зокрема.

Розглянуто основні методи системного аналізу безпеки об’єктів.

Проведено аналіз методів автентифікації користувачів.

Описано особливості розробки інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури.

Описано архітектуру ресурсу, а також систему безпеки від несанкціонованого доступу, обмеження доступу до даних в залежності від ролі користувача.

Проведена розробка і реалізація бази даних.

Реалізовано систему аналізу безпеки аналітиком, розроблений модуль додаткового захисту, досліджено результати її роботи.

Проаналізовано необхідні економічні показники, проведені відповідні розрахунки, з’ясовано економічну доцільність розробки і її комерційний потенціал.

# ANNOTATION

Bilous V.M.. Development of a protected consolidated information resource of a system analysis of the security of the information and telecommunication infrastructure of the region. Master's qualification thesis on specialty 125 - "Cybersecurity", educational program "Cybersecurity of information technologies and systems". Vinnytsia: VNTU, 2023. 135 p.

In the Ukrainian language. Bibliography: 63 titles; Fig.: 16; table 13.

The purpose of the master's work is to develop a protected consolidated information resource of a system analysis of the security of the information and telecommunication infrastructure of the region.

The security features of critical infrastructure facilities in general and information and telecommunication infrastructure in particular have been clarified.

The main methods of system analysis of object security are considered.

An analysis of user authentication methods was carried out.

Features of the development of an information resource for information and telecommunication infrastructure security analysis are described.

The resource architecture is described, as well as the security system against unauthorized access, data access restrictions depending on the user's role.

The database was developed and implemented.

The security analysis system was implemented by the analyst, the additional protection module was developed, and the results of its work were studied.

The necessary economic indicators were analyzed, relevant calculations were made, the economic feasibility of the development and its commercial potential were clarified.

**ЗМІСТ**

# ВСТУП

**Актуальність теми.** Інформаційно-телекомунікаційна інфраструктура (ІТІ) - це сукупність технічних, організаційних, програмних та людських ресурсів, які забезпечують заходи по передачі, обробці і зберіганню необхідної інформації, а також забезпечують комунікаційні можливості між різними точками мережі.

Тема безпеки інформаційно-телекомунікаційної інфраструктури є надзвичайно актуальною в сучасному світі. Зростання використання інформаційних технологій, а також, залежність від цифрової інфраструктури робить цю тему все більш важливою.

Одна з головних причин актуальності цієї теми - зростання кількості кібератак і кіберзлочинності. У нашому цифровому світі, де всі наші особисті дані, фінансова інформація та комунікації зберігаються і передаються в електронній формі, злочинцям стає все простіше здійснювати атаки на цю інформацію. Це може призвести до витоку особистих даних, фінансових втрат і порушення довіри до електронних сервісів та телекомунікацій.

Інший фактор, що підвищує актуальність цієї теми - це залежність економіки від безпечного функціонування інформаційно-телекомунікаційної інфраструктури.

Консолідований інформаційний ресурс аналізу безпеки інформаційно-телекомунікаційної інфраструктури допоможе проводити аудит критичних об’єктів і аналізувати їх безпеку, що дозволить аналітикам отримати цілісний погляд на безпековий стан галузі.

**Мета дослідження.** Дослідження методів оцінювання безпекового стану критичних об’єктів інформаційно-телекомунікаційної інфраструктури, розробка консолідованого інформаційного ресурсу для аналізу їх безпеки.

**Задачі дослідження:**

1. Аналіз методів системного аналізу безпеки об’єктів.

2. Визначення безпекових загроз критичних об`єктів інформаційно-телекомунікаційної інфраструктури.

3. Розробка архітектури, створення бази даних і забезпечення захисту.

4. Розробка функціоналу і алгоритмів обробки та аналізу інформації про безпеку об’єктів інформаційно-телекомунікаційної інфраструктури.

5. Розробка аналітичної звітності, як результату аналізу безпекових даних об`єктів.

6. Розрахунок економічних показників розробки.

**Об’єкт дослідження.** Об’єктом дослідження є стан безпеки інформаційно-телекомунікаційної інфраструктури.

**Предмет дослідження.** Теоретичні і практичні заходи реалізації консолідованого ресурсу.

**Наукова новизна.** Вперше розроблено захищений консолідований інформаційний ресурс аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону, що надає можливість вирішення проблеми комплексного аналізу безпеки її критичних об’єктів для більш ефективного забезпечення безпеки.

**Практична цінність.** Створений консолідований інформаційний ресурс аналізу безпеки інформаційно-телекомунікаційної інфраструктури, який дозволяє аналітику отримати аналітичні дані про безпековий стан об’єктів критичної інфраструктури і зробити висновки щодо ступеня їх захищеності.

За тематикою роботи опубліковано 3 публікації, зокрема 1 статтю у фаховому виданні та 2 тези доповідей на наукових конференціях [61–63].

# РОЗДІЛ І. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 1.1 Загальні положення про безпеку критичної інфраструктури

Актуальність забезпечення безпеки критичних об'єктів є надзвичайно важливою, оскільки ці об'єкти є стратегічно важливими для держави та суспільства в цілому. Вони забезпечують життєдіяльність населення, економічну стійкість та безпеку країни.

Критична інфраструктура - це сукупність об'єктів, систем і процесів, які є життєво важливими для функціонування суспільства, національної економіки і безпеки країни. Вона включає в себе такі сектори, як енергетика, транспорт, водопостачання, комунікації, фінанси, охорона здоров'я, інформаційні технології, харчова промисловість, система захисту, комунальні послуги тощо. Критична інфраструктура є вразливою до природних катастроф, техногенних аварій, кібератак, терористичних актів та інших загроз. Захист і забезпечення безперебійної роботи критичної інфраструктури є важливим завданням для забезпечення безпеки суспільства та функціонування держави [1].

Критична інфраструктура є важливою для забезпечення повсякденного життя громадян, економічного розвитку, національної безпеки і вимог конкурентоспроможності. Її порушення або відмова можуть мати серйозні наслідки для функціонування суспільства та спричинити значні збитки.

Захист критичної інфраструктури включає в себе розробку та впровадження заходів проти природних катастроф, техногенних аварій, кібератак та терористичних актів. Це можуть бути зміцнення будівель, створення резервних систем, налагодження постійного моніторингу та контролю, розробка планів управління кризовими ситуаціями, проведення тренувань та навчань персоналу.

Держави розробляють стратегії та програми забезпечення безпеки критичної інфраструктури, співпрацюють з приватними компаніями та іншими заінтересованими сторонами для ризик-оцінки, планування запобігання та

реагування на можливі загрози. Основні принципи захисту критичної інфраструктури включають прозорість, координацію, співпрацю та забезпечення обміну інформацією між відповідними структурами та органами влади.

Можна виділити 3 рівня критичної інфраструктури (рисунок 1.1):


Рисунок 1.1 - Рівні критичної інфраструктури

Захист критичної інфраструктури - це незрозумілий і постійний процес, оскільки загрози постійно змінюються і еволюціонують. Дотримання стандартів безпеки, інвестиції в нові технології та інновації, технічний розвиток та постійний аналіз ризиків є важливими елементами успішного захисту критичної інфраструктури.

Критична інфраструктура також може бути поділена на дві основні категорії: фізична і кіберінфраструктура.

Фізична критична інфраструктура включає будівлі, споруди, мережі, обладнання і системи, які забезпечують життєво важливі послуги. Наприклад,

енергетичні станції, мережі електропостачання, водопостачання та каналізації, транспортна інфраструктура, така як аеропорти, морські порти, залізниці і автодороги, а також системи зв'язку, комунікацій та інтернету.

Кіберінфраструктура включає в себе інформаційні системи та мережі, комп'ютерні системи, сховища даних, програмне забезпечення і інші технологічні компоненти, які забезпечують обробку, зберігання і передачу інформації. Зокрема, це можуть бути урядові системи, мережі банків і фінансових установ, системи управління транспортом, системи забезпечення охорони здоров'я, критичні підприємства і інші системи, які є основою економіки та суспільства.

Забезпечення захисту критичної інфраструктури є важливим завданням національної безпеки. Держави розробляють стратегії, політику та нормативно-правову базу для захисту критичної інфраструктури. Це включає в себе удосконалення технологій і софтверу для виявлення і запобігання кібератакам, проведення тренувань і навчань працівників, резервне копіювання та відновлення даних, а також забезпечення міжнародного співробітництва в цій сфері.

Усвідомлення важливості захисту критичної інфраструктури стає все більш актуальним, оскільки сучасні загрози стають все більш складними і субтильними. Перевага належить тим, хто виявляє проникну атаку або загрозу до критичної інфраструктури, тому важливо не лише реагувати, але й передбачати, запобігати та забезпечувати належний рівень захисту критичної інфраструктури.

Критична інфраструктура також може бути поділена на різні підсистеми залежно від свого призначення та важливості. Наприклад:

1. Енергетична інфраструктура: це включає системи виробництва, передачі і розподілу електроенергії, газу і нафти. Ця інфраструктура є ключовою для забезпечення енергії для побутових, комерційних та промислових потреб.

2. Транспортна інфраструктура: це включає автомагістралі, залізниці, аеропорти, морські порти та інші об'єкти, які забезпечують перевезення товарів та людей. Ця інфраструктура виконує важливу роль у забезпеченні мобільності і зближення різних регіонів.

3. Комунальна інфраструктура: це включає системи водопостачання, каналізації, вивезення сміття та інші комунальні послуги. Ця інфраструктура є важливою для забезпечення життєвих умов і добробуту населення.

4. Інформаційно-комунікаційна інфраструктура: це включає системи зв'язку, телефонії, комп'ютерні мережі та інші технології, що забезпечують обмін інформацією. Ця інфраструктура є основою сучасного суспільства та бізнесу, і без неї неможливо функціонування багатьох інших секторів [2].

Недостатність, злам або відмова в роботі будь-якої з цих підсистем критичної інфраструктури може призвести до серйозних наслідків, таких як простої виробництва, відсутність енергопостачання, зупинка транспорту, забруднення питної води і тому подібне. Тому, забезпечення захисту, стійкості і безперебійності цих систем є ключовим завданням для забезпечення безпеки суспільства і збереження його функціонування в кризових ситуаціях.

Для додаткового розуміння критичної інфраструктури, можна розглянути деякі приклади конкретних об'єктів і систем, які входять до цієї категорії:

1. Ядерні електростанції: Ядерні електростанції є складними інженерними спорудами, призначеними для виробництва електроенергії. Пошкодження або відмова в роботі ядерної електростанції може мати руйнівний вплив на людей і навколишнє середовище. Тому їх захист, безпека і запобігання можливим аваріям є надзвичайно важливими.

2. Комунікаційна мережа: Це включає мобільні та проводові телефонні мережі, інтернет-провайдерів і супутникові зв'язку. Ці мережі є ключовими для комунікації між людьми, передачі даних, електронної комерції і багатьох інших аспектів сучасного життя та бізнесу.

3. Фінансова і банківська системи: Банки, фінансові установи та платіжні системи також входять до критичної інфраструктури. Ці системи забезпечують фінансові операції, обмін валют, переказ грошей та інші фінансові послуги. Злам або відмова в роботі цих систем може спричинити фінансову нестабільність і серйозні економічні наслідки.

4. Системи водопостачання та водоочищення: Ці системи забезпечують доступ до чистої питної води та водопостачання для господарських потреб. Порушення роботи цих систем може спричинити відсутність води або появу забрудненої води, що становить серйозну загрозу для здоров'я та гігієни людей.

Критична інфраструктура відіграє важливу роль у суспільстві, економіці та безпеці країни. Захист цих систем стає все більш складним і вимагає постійної уваги, інвестицій у технології та заходи безпеки. Відповідні організації, урядові органи та приватні компанії співпрацюють для забезпечення безперебійності та стійкості критичної інфраструктури.

Особливості забезпечення безпеки об'єктів критичної інфраструктури полягають у врахуванні специфічних ризиків, зокрема, природних катастроф, техногенних аварій, кібератак та терористичних актів. Врахування цих ризиків передбачає розробку та реалізацію комплексних заходів з попередження, виявлення та ліквідації загроз.

Основні засади забезпечення безпеки об'єктів критичної інфраструктури включають [7-12]:

1. Оцінка ризиків. Проведення систематичного аналізу потенційних загроз та визначення рівня вразливості об'єкту.

2. Превентивні заходи. Розробка та впровадження превентивних заходів, які спрямовані на зменшення можливості виникнення загроз та мінімізацію їх можливих наслідків.

3. Виявлення та реагування. Створення систем виявлення та реагування на загрози безпеці, включаючи моніторинг, виявлення вторгнень та пошук і нейтралізацію загроз.

4. Взаємодія та координація. Забезпечення ефективної взаємодії між відповідальними структурами та організаціями, а також координація їх дій для ефективного ліквідації загроз безпеці.

5. Комплексна оцінка впливу. Врахування потенційного впливу загроз на соціально-економічну сферу, довкілля та безпеку населення. Це включає здатність визначити розмір, масштаб та тривалість можливих наслідків загроз.

6. Постійне навчання та підвищення кваліфікації персоналу. Надання спеціального навчання та підготовки персоналу об'єктів критичної інфраструктури з питань безпеки, включаючи навички управління кризовими ситуаціями та дотримання стандартів безпеки.

7. Захист інформації. Забезпечення захисту інформації про об'єкти критичної інфраструктури від несанкціонованого доступу, крадіжок та кібератак. Це включає впровадження захисних технологій, контроль доступу та обмеження використання конфіденційної інформації.

8. Партнерство з галузевими гравцями. Співпраця з приватними суб'єктами, власниками та операторами об'єктів критичної інфраструктури для спільного забезпечення безпеки. Це може включати розробку спільних планів надзвичайних ситуацій, обмін інформацією та ресурсами, а також регулярні перевірки безпеки об'єктів.

9. Постійне вдосконалення і тестування систем безпеки. Регулярне оновлення та перевірка ефективності заходів забезпечення безпеки, а також проведення планових перевірок і навчань для персоналу і робочих груп.

Забезпечення безпеки об'єктів критичної інфраструктури є постійним процесом і вимагає постійного моніторингу, оновлення та удосконалення заходів з метою виявлення та запобігання новим ризикам і загрозам.

Взаємодія суб'єктів безпеки, впровадження інноваційних технологій та постійне вдосконалення систем забезпечення безпеки об'єктів критичної інфраструктури є ключовими передумовами для ефективного захисту цих об'єктів від потенційних загроз і забезпечення стійкості та безпеки країни.

Однією з особливостей забезпечення безпеки об'єктів критичної інфраструктури є необхідність працювати в режимі 24/7. Оскільки ці об'єкти є важливими для життєдіяльності суспільства, забезпечення їх безпеки не може бути припинене чи обмежене в певний відрізок часу. Тому об'єкти критичної інфраструктури повинні мати постійно діючі системи нагляду, виявлення і реагування на загрози та кризових ситуацій.

Далі, забезпечення безпеки об'єктів критичної інфраструктури вимагає високої стійкості до ситуацій надзвичайного характеру. Це включає врахування можливості природних катастроф, відмов технічних систем, кібератак та інших факторів, які можуть спричинити зупинку або значні перебої в роботі об'єкту. Тому безпека об'єктів критичної інфраструктури повинна базуватися на резервуванні, забезпеченні надійності та відновлюваності систем, а також проведенні систематичних аудитів безпеки.

Також варто відзначити, що критичні інфраструктурні об'єкти можуть містити генеруючі, зберігаючі та оброблюючі критичні дані. Тому безпека об'єктів критичної інфраструктури передбачає захист інформації та використання захищених засобів збереження і передачі даних.

Загалом, безпека об'єктів критичної інфраструктури - це складне завдання, яке вимагає комплексного підходу і залучення мультидисциплінарних експертів. Врахування актуальних загроз та розвиток адекватних стратегій та заходів забезпечення безпеки дозволять зменшити ризики і зберегти функціонування об'єктів критичної інфраструктури навіть у найскладніших ситуаціях.

Об’єкти інфраструктури класифікують за категоріями критичності, яка є критерієм оцінки важливості такого об’єкту [3]:

- категорія I (особливо важливі) - об’єкти загальнодержавного значення, які мають великий вплив на інші об’єкти критичної інфраструктури. Збої в їх роботі можуть призвести до кризової ситуації на рівні держави;
- категорія II (життєво важливі) – порушення роботи яких призводить до кризової ситуації на рівні регіону;
- категорія III (важливі) – порушення роботи яких призводить до кризової ситуації на місцевому рівні;
- категорія IV (локальні) – збої в роботі призводять до виникнення кризової ситуації локального значення.

Основні види безпек [3]:

- фізична безпека – заходи, які спрямовані на унеможливлення або припинення фізичних актів втручання;

- кібербезпека - безпека інформації і інформаційно-телекомунікаційних систем.

За забезпечення фізичної і кібербезпеки відповідає оператор критичної інфраструктури.

Оператор критичної інфраструктури - юридична особа або фізична особа - підприємець (ФОП), що здійснює управління цим об’єктом і відповідає за його безпековий стан.

Кібербезпека має цикл управління, що складається з 5 ключових функцій, які виконуються послідовно – ідентифікація ризиків, кіберзахист, виявлення інцидентів, реагування та відновлення нормального стану [4] (рисунок 1.2).


Рисунок 1.2 – Цикл управління кібербезпекою

Існують 4 рівні впровадження кіберзахисту [4]:

1. частковий - практика кіберзахисту існує, але вона не є формалізованою, обмежене розуміння ризиків, власник ОКІ не розуміє місце та роль ОКІ у системі забезпечення кібербезпеки сектору інфраструктури;

2. ризик-орієнтований - практика кіберзахисту впроваджується, але не є інституціональною, ризики кібербезпеки розуміються, але немає формалізованого процесу управління ризиками, оператор ОКІ взаємодіє з іншими об'єктами, але процеси взаємодії не є формалізованими;
3. повторюваний - практика кіберзахисту інституціоналізована, впроваджено загально-організаційний підхід до управління ризиками кібербезпеки, взаємодія з іншими ОКІ формалізована та інституціоналізована;
4. адаптивний - практика кіберзахисту адаптується на основі практичного досвіду та прогнозованих показників безпеки. Управління ризиками кібербезпеки є частиною організаційної культури та розвивається на основі усвідомлення попередньої діяльності з управління ризикамита постійної обізнаності про діяльність із забезпечення кібербезпеки. Взаємодія здійснюється на постійній основі, інформація про стан кібербезпеки використовується в реальному часі.

Ці рівні мають ієрархічну структуру, при виборі враховується характеристики загроз, поточний стан реалізації заходів кібербезпеки, управління ризиками, вимоги законодавства, обмеження.

Після успішного досягнення конкретного рівня впровадження рекомендовано покращувати заходи кібербезпеки з перспективою переходу на наступний рівень.

Для забезпечення безпеки об’єктів критичної інфраструктури можна виділити такі основні завдання [5-6]:

1. Виявлення потенційних загроз і ризиків. Це може включати вивчення потенційних загроз, аналіз історичних даних та прогнозування можливих сценаріїв загроз.

2. Забезпечення фізичної безпеки. Це включає контроль доступу до об'єктів, встановлення систем відеоспостереження, охоронну сигналізацію, пожежну

сигналізацію та інші заходи, що запобіганють несанкціонованому доступу та фізичному пошкодженню інфраструктури.

3. Забезпечення кібербезпеки. Це включає розробку та впровадження заходів для захисту інформаційних систем від кібератак, таких як віруси, хакерські атаки та кібершпигунство.

4. Реагування на надзвичайні ситуації. Це включає планування та підготовку до надзвичайних подій, включаючи навчання персоналу, проведення випробувань систем управління кризовими ситуаціями та координацію з іншими органами безпеки.

5. Забезпечення безпеки персоналу. Це включає навчання персоналу з питань безпеки, протидії тероризму, пожежної безпеки, першої медичної допомоги, захисту інформації та інших аспектів забезпечення безпеки, а також забезпечення відповідного обладнання і ресурсів для аварійних ситуацій. Постійне навчання допомагає підтримувати високий рівень готовності персоналу та забезпечує ефективну реакцію на будь-які загрози.

6. Забезпечення безпеки життєзабезпечення. Це включає забезпечення безперебійного функціонування систем забезпечення енергії, водопостачання, транспорту та інших важливих систем, щоб забезпечити безпеку та життєздатність населення.

7. Безпека мереж і комунікацій. Це включає захист мережевої інфраструктури, включаючи маршрутизатори, комутатори, сервери та інші мережеві компоненти. Також слід забезпечити безпеку мобільних зв'язків та інтернет-з'єднань, щоб уникнути можливості хакерських атак або перехоплення конфіденційної інформації.

8. Моніторинг та виявлення аномальних дій. Це включає встановлення систем моніторингу, які відстежують активність на об'єкті та виявляють будь-які підозрілі або незвичайні дії. Це дозволяє оперативно реагувати на потенційні загрози та негайно вживати заходи для їх запобігання.

9. Контроль і аудит систем безпеки. Це включає періодичний аналіз та оцінку ефективності систем безпеки, проведення аудиту та виявлення слабких місць, а також впровадження виправних заходів для посилення безпеки.

10. Контингентний планування та відновлення після кризових ситуацій. Це включає розробку та впровадження планів дій у разі виникнення кризових ситуацій, а також проведення вправ і навчання персоналу для ефективного реагування і відновлення після подій.

11. Сертифікація та стандартизація безпекових заходів. Це включає визначення стандартів та вимог щодо забезпечення безпеки об'єктів критичної інфраструктури, а також сертифікацію систем та технологій, що використовуються для забезпечення безпеки. Це сприяє підвищенню якості та надійності заходів забезпечення безпеки.

12. Економічне оцінювання ризиків та вибір оптимальних заходів. Це включає розрахунок економічного ефекту заходів забезпечення безпеки та вибір оптимальних технічних та організаційних заходів забезпечення безпеки, з урахуванням фінансових обмежень та ризиків.

13. Співпраця з владними та правоохоронними органами. Це включає активну співпрацю з владними органами, поліцією, спеціальними службами та іншими схваленими організаціями, що займаються безпекою. Це допомагає виявляти і розслідувати потенційні загрози, а також забезпечує ефективну координацію у разі надзвичайної ситуації.

Ці завдання не є вичерпними, але вони представляють основні аспекти забезпечення безпеки об'єктів критичної інфраструктури. Завдання можуть розрізнятися залежно від конкретного об'єкта та його функціональності і мають на меті забезпечення надійного та безпечного функціонування об'єктів критичної інфраструктури і захисту від потенційних загроз. Реалізація цих завдань вимагає комплексного підходу та постійного оновлення заходів забезпечення безпеки відповідно до загроз та вимог, які змінюються.

## 1.2 Особливості інформаційно-телекомунікаційної інфраструктури

Телекомунікаційна мережа - це система передачі та обміну інформацією, що включає в себе різні засоби комунікації, такі як телефонні лінії, мобільні мережі, комп'ютерні мережі, супутникові системи зв'язку та інші. Вона забезпечує передачу голосу, даних, відео, зображень іншими засобами та відстань. Телекомунікаційні мережі використовуються в різних сферах, таких як комунікація між користувачами, широкомасштабні мережі для передачі даних та забезпечення стабільного доступу до інтернету, телекомунікаційні підприємства, мережі зв'язку між установами та багато іншого.

Інформаційно-телекомунікаційна інфраструктура (ІТІ) - це система, що включає в себе різноманітні технологічні засоби, мережі, програмні продукти, обладнання, послуги та людські ресурси, які необхідні для забезпечення передачі, обробки, зберігання та використання інформації у великому масштабі.

ІТІ дозволяє підключати людей, організації, комп'ютери та інші пристрої з метою обміну інформацією, комунікації, зберігання даних та доступу до різних сервісів і ресурсів. Вона є основною складовою частиною сучасного інформаційного суспільства і допомагає поліпшити доступ до інформації, здійснювати комунікацію, виконувати різноманітні завдання та послуги швидше і ефективніше.

Інформаційно-телекомунікаційна інфраструктура включає в себе комплекс технологій, ресурсів і інфраструктурних засобів, що забезпечують обмін інформацією та зв'язок між користувачами. Ця область включає в себе телекомунікаційні мережі, обчислювальні системи, програмне забезпечення, обробку даних, системи зберігання інформації, а також апаратне забезпечення.

Основною метою інформаційно-телекомунікаційної інфраструктури є забезпечення надійного доступу до інформації та ефективного обміну даними між різними користувачами. Вона є необхідною для розвитку сучасного суспільства і має великий вплив на економіку, науку, освіту, медицину, транспорт і інші сфери життя.

Основні компоненти інформаційно-телекомунікаційної інфраструктури включають:

1. Телекомунікаційні мережі: це системи передачі і обміну даними, що забезпечують зв'язок між різними пристроями і користувачами. Вони можуть бути провідними (наприклад, телефонні лінії) або бездротовими (наприклад, мобільний зв'язок).

2. Обчислювальні системи і сервери: це апаратне і програмне забезпечення, що забезпечує обробку даних і виконання різних завдань.

3. Системи зберігання інформації: це пристрої і технології для зберігання інформації, такі як сервери, диски, хмарні системи.

4. Програмне забезпечення: це набір програм і додатків, що дозволяють користувачам обробляти інформацію, спілкуватися, робити операції тощо.

5. Інформаційні системи: це системи, що забезпечують збір, обробку і аналіз даних для розв'язання певних завдань.

6. Комп'ютерні мережі: це мережі, що об'єднують комп'ютери і пристрої для обміну даними і ресурсами.

Важливим аспектом інформаційно-телекомунікаційної інфраструктури є забезпечення безпеки і захисту інформації, оскільки вона несе велику кількість важливих і конфіденційних даних. Також потрібно забезпечити надійність і стабільність роботи системи, щоб забезпечити безперебійний доступ до інформації.

В умовах ринкової економіки суб'єктами підприємницької діяльності у сфері телекомунікацій є оператори мереж і постачальники послуг (Public Network). Вони забезпечують побудову мереж загального користування, які називаються мережами загального користування, або публічниими мережами, які призначені для надання послуг зв’язку багатьом користувачам у багатьох різних категоріях [13-14].

В цей перелік не входять мережі, які належать приватним компаніям.

Network Operator (мережевий оператор) - це компанія, яка забезпечує послуги зв'язку, такі як мобільна та фіксована телефонія, мобільний Інтернет,

передача даних та інші послуги, шляхом управління і підтримки телекомунікаційних мереж. Мережевий оператор володіє, управляє та підтримує свою власну інфраструктуру, таку як базові станції, комутатори, маршрутизатори та інші обладнання, необхідні для надання послуг зв'язку своїм клієнтам. Ці компанії також можуть укладати договори з іншими операторами для обміну трафіком та підтримки послуг роумінгу.

Мережевий оператор відповідає за планування, розгортання та підтримку своєї телекомунікаційної інфраструктури. Вони встановлюють і управляють базовими станціями, які забезпечують бездротове підключення до мобільної мережі, комутаторами, які керують телефонними лініями та передачею даних, а також маршрутизаторами, які направляють дані по мережі.

Мережеві оператори також забезпечують підтримку та обслуговування своїх абонентів, включаючи надання технічної підтримки та вирішення проблем зі з'єднанням. Вони також виступають посередниками між своїми абонентами та іншими операторами мережі для забезпечення послуг роумінгу та міжоператорського обміну трафіком.

Мережеві оператори можуть працювати на різних ринках телекомунікаційного сектору, включаючи мобільні оператори, фіксовані оператори телефонії, оператори Інтернету та провайдери послуг передачі даних. Вони зазвичай пропонують різні послуги зв'язку, включаючи голосовий зв'язок, SMS-повідомлення, мобільний Інтернет, послуги передачі даних і багато інших.

Основними завданнями мережевого оператора є забезпечення надійного та стабільного зв'язку для своїх абонентів, підтримка мережевої безпеки та конфіденційності даних, а також розробка та впровадження нових технологій та послуг для поліпшення якості зв'язку та задоволення потреб клієнтів.

Мережеві оператори також відповідають за управління мережевим трафіком, балансування навантаження та оптимізацію ресурсів, щоб забезпечити якісне обслуговування своїх клієнтів. Вони мають інструменти та системи, які дозволяють вимірювати та аналізувати якість зв'язку, доступність мережі та

продуктивність, щоб вчасно виявляти проблеми та вживати заходів для їх вирішення.

Також важливою функцією мережевих операторів є підтримка розширення та модернізації мережі, особливо з урахуванням швидкого темпу зростання трафіку та розвитку нових технологій. Вони займаються плануванням інвестицій у нове обладнання, розширення і підвищення ємності мережі, встановлення нових технологій, таких як 5G, для покращення швидкості та якості зв'язку для своїх абонентів.

Мережеві оператори також взаємодіють з регуляторними органами, які встановлюють правила та стандарти для телекомунікаційного сектору. Вони повинні відповідати вимогам та нормам для забезпечення безпеки та якості послуг, захисту прав споживачів та конкуренції на ринку.

Мережевий оператор - це ключовий гравець у сфері телекомунікацій, який забезпечує надійні та сучасні послуги зв'язку для клієнтів і відповідає за управління, розгортання та підтримку телекомунікаційної інфраструктури.

Додатково до своїх основних функцій, мережеві оператори можуть виконувати ще кілька важливих ролей. Деякі з них включають:

1. Реалізація послуги підключення до мережі: Мережеві оператори надають підприємствам та організаціям послуги з підключення до їх телекомунікаційної інфраструктури. Це може охоплювати встановлення та налаштування обладнання, надання необхідної супровідної інфраструктури та забезпечення постійного доступу до мережі.

2. Виконання ролі трафікового обміну: Мережеві оператори можуть встановлювати угоди про трафіковий обмін з іншими операторами з метою забезпечення покриття і зв'язку для своїх абонентів. Це дозволяє передавати дані через різні мережі, забезпечуючи швидкість, надійність та доступність послуг.

3. Управління корпоративними мережами: Деякі мережеві оператори спеціалізуються на наданні послуг корпоративним клієнтам, таким як підприємства та установи. Вони можуть розробляти та керувати мережами

підприємств, забезпечуючи високу продуктивність, безпеку та пропускну здатність для їхніх специфічних потреб.

4. Впровадження нових технологій та інновацій: Мережеві оператори грають важливу роль у впровадженні нових технологій, таких як 5G, інтернет речей (IoT), віртуалізація мережі та інші інноваційні рішення. Вони досліджують та впроваджують нові технології для поліпшення якості зв'язку, покриття та забезпечення нових можливостей для своїх клієнтів.

Мережеві оператори відіграють ключову роль у забезпеченні послуг зв'язку та передачі даних для індивідуальних користувачів і підприємств. Вони забезпечують покриття, швидкість та якість з'єднання, а також впроваджують нові технології, щоб задовольнити зростаючі потреби своїх абонентів.

Законодавство України встановлює ряд вимог щодо діяльності мережевих операторів (Network Operators). Основні вимоги включають:

1. Ліцензування: Україна вимагає, щоб мережеві оператори мали ліцензію на надання послуг зв'язку. Ліцензія видається Національною комісією з питань регулювання зв'язку інформатизації.

2. Захист особистих даних: Мережеві оператори повинні дотримуватися норм законодавства по захисту персональних даних, який встановлює правила щодо збору, зберігання, обробки та передачі персональних даних користувача.

3. Забезпечення безпеки мережі: Мережеві оператори повинні забезпечувати безпеку мережі зв'язку та захист її від несанкціонованого доступу, вірусів, кібератак та інших загроз.

4. Заборона блокування та перешкоджання доступу: Мережеві оператори заборонене здійснювати блокування доступу до інформації, за винятком тих випадків, які визначені законодавством.

5. Забезпечення доступу до послуг зв'язку: Мережеві оператори повинні забезпечувати доступ до послуг зв'язку користувачам без будь-яких форм дискримінації.

6. Відповідальність: Мережеві оператори несуть відповідальність перед законом за порушення встановлених вимог та інших обов'язків.

7. Вимоги до якості послуг: Мережевий оператор повинен забезпечувати якість послуг зв'язку відповідно до встановлених стандартів. Це означає, що оператор повинен забезпечувати надійність, швидкість, доступність та якість передачі даних, голосу та інших послуг зв'язку.

8. Операторські зобов'язання: Мережевий оператор має забезпечувати надання послуг на основі встановлених тарифів та умов, які повинні бути прозорими та доступними для користувачів. Оператор також має надавати реальну можливість користувачам змінювати оператора та/або послугового оператора.

9. Заборона дискримінації: Мережевий оператор не має дискримінувати користувачів за такими ознаками, як національність, раса, колір шкіри, релігійні переконання, інвалідність, політичні переконання або інший соціальний статус.

10. Захист споживачів: Мережевий оператор зобов'язаний розробити процедури та механізми для розгляду скарг та вирішення спорів із споживачами. Вони також повинні забезпечувати право користувачів на інформацію про послуги, тарифи, умови та вимоги, які стосуються їх договору з оператором.

11. Заборона незаконної перешкоди: Мережевий оператор не має незаконно перешкоджати доступу користувачів до послуг інших операторів або послугових операторів. Оператор повинен дотримуватися принципу взаємодії та свободи вибору для користувачів.

12. Працівники та нормативні вимоги: Мережевий оператор повинен забезпечувати належну кваліфікацію своїх працівників, а також дотримуватися всіх нормативних вимог та стандартів безпеки щодо експлуатації та обслуговування мереж.

Враховуючи ці вимоги, мережеві оператори зобов'язані діяти відповідно до закону України та підлягати контролю з боку відповідних регулюючих органів для забезпечення безпеки, якості та захисту прав користувачів.

Internet Service Providing, або професійне надання інтернет-сервісів, - це послуга, яка надається провайдерами для забезпечення доступу користувачів до Інтернету, тому ISP (постачальник сервісів Інтернету) надає підключення до Інтернету для домашніх користувачів, підприємств та інших організацій.

ISP зазвичай пропонують різні види підключень до Інтернету, включаючи провідні (оптичні, кабельні, DSL), бездротові (Wi-Fi, супутникові) і мобільні (3G, 4G, 5G). Вони також можуть надавати інші послуги, такі як пошта електронної пошти, віртуальні приватні мережі (VPN), хостинг та інше.

ISP відповідає за налагодження та підтримку мережі, яка дозволяє користувачам підключатися до Інтернету. Вони також забезпечують безпеку мережі, контролюють трафік та надають технічну підтримку клієнтам. ISP може бути різними компаніями, включаючи телефонні оператори, кабельні компанії, супутникові оператори та інші провайдери послуг зв'язку.

Оскільки інтернет-підключення стало необхідністю для багатьох людей та організацій, ISP грають важливу роль у забезпеченні доступу до Інтернету та забезпеченні якісного та надійного послуги.

ISP забезпечує підключення клієнтів до глобальної мережі Інтернет шляхом використання різних технологій і засобів передачі даних. Вони можуть мати свої власні мережі інфраструктури, які включають сервери, роутери, комутатори та інші обладнання для передачі інформації.

ISP також відповідає за призначення IP-адреси клієнту, яка є унікальним ідентифікатором пристрою в мережі Інтернет. Вони також можуть надавати додаткові послуги, такі як антивірусне програмне забезпечення, фільтрація контенту, хмарне сховище та інші.

ISP зазвичай пропонують різні тарифні плани та пакети послуг залежно від потреб користувачів. Вони можуть надавати швидкісне підключення до Інтернету, обмежене або необмежене використання даних, підтримку телекомунікаційних послуг (наприклад, сім-карти та телефонні дзвінки через Інтернет) та інші опції.

ISP також відповідає за збереження та захист персональних даних користувачів згідно з вимогами захисту конфіденційності та безпеки. Вони повинні дотримуватися різних правил і норм, таких як Закон про захист персональних даних та регуляторні положення, що стосуються надання інтернет-послуг.

Одним із важливих аспектів роботи ISP є якість надання послуг та надійність підключення. Вони повинні забезпечити стабільне і швидке підключення до Інтернету, а також вчасну вирішення технічних проблем та неполадок, які можуть виникнути.

ISP є ключовими учасниками в глобальній мережі Інтернет, забезпечуючи доступ користувачам до всесвітнього вебу та інших послуг, які надає Інтернет. Вони відіграють важливу роль у забезпеченні зв'язку, обміну даними та інформацією у всьому світі.

Додатковою функцією ISP є надання технічної підтримки користувачам. Це означає, що ISP стежить за роботою мережі та інтернет-сервісів, виявляє та виправляє проблеми, які можуть виникати у процесі користування Інтернетом. Користувачі можуть звернутися до служби підтримки ISP для отримання допомоги зі з'єднанням, налаштуваннями, відновленням паролів або вирішенням інших технічних питань.

ISP також можуть надавати додаткові послуги, які допомагають забезпечити безпеку та контроль використання Інтернету. Наприклад, вони можуть надати фільтрацію контенту, яка допомагає блокувати доступ до небажаних або шкідливих веб-сайтів. Також можуть бути надані послуги віртуальних приватних мереж (VPN), які забезпечують безпеку та приватність підключення до Інтернету, особливо у випадках використання незахищених мереж.

У деяких випадках ISP можуть обслуговувати великі корпорації або організації, надаючи їм високошвидкісне і надійне підключення до Інтернету. Такі ISP можуть надати спеціалізовані послуги для підтримки багатокористувацьких мереж, обробки великого обсягу даних та інших вимог специфічної сфери діяльності клієнта.

Загалом, ISP є основною складовою частиною інфраструктури Інтернету, яка забезпечує доступ до Інтернету для мільйонів користувачів. Вони грають важливу роль у забезпеченні безпеки, стабільності та якості підключення до мережі і допомагають користувачам вибрати оптимальні послуги відповідно до їхніх потреб і вимог.

Встановлені законодавчі вимоги до ISP, які регулюють їх діяльність і забезпечують безпеку та конфіденційність інтернет-користувачів. Основні вимоги законодавства України до ISP включають:

1. Ліцензування: ISP повинні мати ліцензію, яка дає їм право надавати послуги Інтернету на території України. Це дозволяє державі контролювати діяльність ISP та забезпечувати їх відповідність законодавству.

2. Захист персональних даних: ISP повинні забезпечувати захист персональних даних своїх користувачів, зокрема від доступу третіх осіб. Вони повинні дотримуватися вимог, встановлених Законом України "Про захист персональних даних", і забезпечувати безпечну обробку і збереження інформації про своїх клієнтів.

3. Безпека мережі: ISP повинні приймати заходи для забезпечення безпеки своїх мереж та запобігання несанкціонованому доступу до них. Вони повинні мати захисні механізми, які виявляють та блокують загрози безпеці мережі, такі як віруси, зловмисне програмне забезпечення і хакерські атаки.

4. Спостереження за трафіком: ISP можуть зобов'язані зберігати дані про трафік, який проходить через їх мережу, протягом певного періоду часу. Це виконується з метою забезпечення безпеки, розслідування правопорушень та виконання декретів суду.

5. Дотримання авторських прав: ISP повинні запобігати порушенню авторських прав через свою мережу. Вони повинні співпрацювати з власниками авторських прав і приймати заходи для блокування або виключення доступу до порушувачів прав.

6. Загальний доступ до Інтернету: ISP не повинні обмежувати доступ користувачів до Інтернету без законного підстави. Вони не мають права забороняти доступ до веб-сайтів або послуг, які не суперечать законодавству.

7. Співпраця з правоохоронними органами: ISP повинні співпрацювати з правоохоронними органами та надавати їм необхідну інформацію для розслідування правопорушень. Вони повинні також допомагати у виконанні рішень суду, якщо це не суперечить законодавству.

8. Блокування незаконного контенту: ISP повинні приймати заходи для блокування незаконного контенту, включаючи дитячу порнографію, розповсюдження насильства та ненависті, пропаганду тероризму тощо. Вони повинні дотримуватися блокування відповідно до вимог законодавства про телебачення і радіомовлення та іншого законодавства.

9. Запобігання кібератакам: ISP повинні вживати заходів для запобігання кібератакам та виявлення і ліквідації їх наслідків. Вони повинні мати механізми для виявлення зловмисних активностей, включаючи DDoS-атаки, фішинг та інші загрози безпеці.

10. Обмеження пропаганди: ISP повинні дотримуватися Закону України "Про забезпечення права на доступ до публічної інформації" та приймати заходи для обмеження пропаганди, яка веде до насильства, расизму, дискримінації та інших негативних наслідків.

11. Забезпечення невідкладного доступу до інформації: ISP повинні забезпечувати невідкладний доступ до інформації в разі загрози національній безпеці, громадському порядку чи збереженні життя індивіда. Вони можуть отримати виклик від правоохоронних органів або державних служб і мають забезпечити негайне надання необхідної інформації.

12. Співпраця з іншими ISP: ISP повинні співпрацювати між собою із метою забезпечення безпеки та ефективності маршрутизації трафіку. Вони можуть обмінюватися інформацією про загрози, спільно виявляти і вирішувати проблеми, а також координувати роботу національних мереж для забезпечення сталої роботи Інтернету.

Загалом, вимоги законодавства України до ISP спрямовані на забезпечення безпеки, конфіденційності та свободи доступу до Інтернету для користувачів. ISP повинні дотримуватися цих вимог і співпрацювати з державою та іншими сторонами для створення безпечного та доступного цифрового середовища.

Ці вимоги допомагають забезпечити безпеку та права користувачів Інтернету в Україні та сприяють розвитку безпечного та ефективного цифрового середовища

## 1.3 Аналіз методів системного аналізу безпеки критичної інфраструктури

Системний аналіз безпеки об’єктів включає в себе використання різних методів для вивчення та оцінки рівня безпеки об’єктів. Нижче наведені деякі з найпоширеніших методів системного аналізу безпеки об’єктів [22-36].

1. Аналіз загроз. Цей метод включає ідентифікацію потенційних загроз безпеці об’єкта, їх категоризацію та оцінку вірогідності їх виникнення. Для цього можуть використовуватись різні підходи, наприклад, історичний аналіз подій, експертна оцінка та інші методи дослідження.

2. Аналіз уразливостей. Цей метод включає виявлення потенційних уразливостей безпеки об’єкта, їх систематичну класифікацію та оцінку рівня важкості їх використання з боку потенційного зловмисника. Для цього можуть використовуватись різні методи, такі як аналіз вразливостей програмного забезпечення, аналіз критичності комунікаційних мереж та інші.

3. Оцінка ризику. Цей метод включає визначення ризику внаслідок потенційних загроз та уразливостей об’єкта безпеки. Для оцінки ризику можуть використовуватись різні підходи, такі як аналіз імовірності виникнення загрози та аналіз впливу загрози на об’єкт безпеки.

4. Розробка заходів безпеки. Цей метод включає розробку та впровадження заходів безпеки для запобігання або зменшення ризику безпеки об’єкта. Для цього можуть використовуватись різні підходи, такі як встановлення фізичних та технічних заходів безпеки, розробка політики безпеки та інші.

5. Виконання аудиту безпеки. Цей метод включає періодичну перевірку та оцінку рівня безпеки об’єкта з метою виявлення можливих проблем та встановлення відповідних заходів для їх усунення. Для цього можуть використовуватись різні підходи, такі як аудит системи безпеки, регулярні тестування безпеки та ін.

6. Моделювання системи безпеки. Цей метод включає створення математичних або комп'ютерних моделей системи безпеки об'єкта для аналізу

потенційних загроз та оцінки ефективності заходів безпеки. Моделювання дозволяє прогнозувати можливі наслідки і визначати найбільш ефективні стратегії безпеки.

7. Аналіз витрат та бенефітів. Цей метод включає вивчення вартості реалізації заходів безпеки та оцінку їх потенційних вигод. Це може включати витрати на обладнання, навчання персоналу, а також оцінку можливих збитків, що можуть статися у випадку порушення безпеки об'єкта.

8. Моніторинг та інцидентний менеджмент. Цей метод включає систематичне спостереження за безпекою об'єкта та реагування на виявлені проблеми чи порушення. Моніторинг може включати в себе використання систем виявлення вторгнень, планування та впровадження системи реагування на інциденти, а також аналіз та вдосконалення процесів безпеки.

9. Аналіз правового середовища. Цей метод включає вивчення правового середовища, в якому функціонує об'єкт безпеки, з метою визначення його впливу на безпеку. Аналіз правового середовища дозволяє виявити необхідність дотримання певних норм та стандартів, а також оцінити ризики їх порушення.

10. Соціально-психологічний аналіз. Цей метод включає вивчення соціальних та психологічних аспектів безпеки об'єкта. Він дозволяє враховувати взаємодію між людьми та їхнім сприйняттям безпеки, а також ідентифікувати потенційні поведінкові аспекти, що можуть вплинути на безпеку об'єкта.

11. Аналіз бізнес-процесів. Цей метод включає вивчення бізнес-процесів об'єкта з метою виявлення можливих загроз безпеці та відповідних заходів для їх усунення. Аналіз бізнес-процесів може включати ідентифікацію критичних точок та встановлення механізмів контролю та нагляду.

12. Соціальний інжиніринг. Цей метод включає дослідження та аналіз психологічних маніпуляцій та інженерних технік, що використовуються зловмисниками для зламу системи безпеки. Соціальний інжиніринг дозволяє виявити потенційні ризики обману та встановити заходи для їх запобігання.

13. Аналіз стійкості. Цей метод включає аналіз стійкості системи безпеки об'єкта до потенційних атак та зламу. Він оцінює ефективність заходів безпеки та їх здатність запобігти, виявити та відновити систему після нападу.

Ці методи системного аналізу безпеки об'єктів є лише деякими з можливих. Вибір методів залежить від конкретного контексту, функціонального призначення об'єкта та особливостей його безпеки.

Ці методи системного аналізу безпеки об'єктів спрямовані на комплексне вивчення та оцінку безпеки, а також на розробку відповідних заходів для її покращення. Вони можуть бути використані як окремо, так і в поєднанні, залежно від конкретних потреб та вимог об'єкта безпеки.

Аналіз загроз - це процес виявлення, оцінки та опису потенційних загроз, які можуть спричинити негативні наслідки для певної системи, організації або проекту. Загрози можуть виникати з різних джерел, таких як природні стихійні лиха, технічні несправності, зломи безпеки, людські помилки, зловмисні дії та інші.

Процес аналізу загроз зазвичай включає наступні кроки:

1. Виявлення загроз: ідентифікація можливих загроз, які можуть вплинути на систему або організацію. Цей етап може включати прогнозування майбутніх загроз на основі аналізу попередніх випадків або використання спеціалізованого програмного забезпечення.

2. Оцінка загроз: оцінка потенційного впливу кожної загрози на систему або організацію. Це може включати визначення ймовірності виникнення загрози та потенційного збитку, який вона може заподіяти.

3. Опис загроз: детальне описання кожної виявленої загрози, включаючи її характеристики, можливі наслідки та рекомендації щодо запобігання або мінімізації впливу загрози.

Після проведення аналізу загроз, організація може прийняти відповідні заходи для зменшення ризику від загрози, включаючи розробку та впровадження планів контролю та управління випадками негативного впливу. Ці заходи можуть

включати усунення вразливостей системи, вдосконалення технічних захистів, навчання персоналу з питань безпеки та інші.

4. Приоритизація загроз: на основі оцінки загроз і їх впливу, необхідно визначити пріоритети для захисту системи або організації. Це допоможе визначити, які загрози потребують негайного управління і які можуть бути вирішені на наступних етапах.

5. Розробка планів контролю загроз: на основі виявлених загроз і їх оцінки, необхідно розробити плани дій для запобігання або впровадження заходів з контролю над ними. Це може включати впровадження технологічних рішень, зміни процесів або політик.

6. Моніторинг і оновлення: процес аналізу загроз не є статичним і повинен проводитись упродовж часу. Загрози можуть змінюватись, нові загрози можуть з'являтись, а існуючі загрози можуть ставати більш складними. Тому, процес аналізу загроз повинен бути відновлюваним і систематичним.

Загальний аналіз загроз допомагає організаціям або проектам розуміти потенційні пам'ятати ризиків і забезпечувати належний рівень захисту. Ця інформація може використовуватись для розробки стратегій управління ризиками, додаткових інвестицій для захисту та інших прийняття рішень, які допоможуть зменшити вплив загроз на систему або організацію.

7. Оцінка вразливостей системи: важливим кроком в аналізі загроз є виявлення вразливостей у системі або організації, які можуть бути використані загрозами для здійснення атак. Це можуть бути слабкі місця у фізичній інфраструктурі, програмному забезпеченні, мережі або людях.

8. Розробка стратегій запобігання і відповіді на загрози: на основі виявлених загроз і вразливостей, потрібно розробити стратегії, що дозволять попередити атаки та зменшити їх вплив. Це може включати застосування сучасних технологій безпеки, розробку політик і процедур безпеки, навчання персоналу та розробку планів відновлення після інциденту.

9. Моніторинг і виявлення вторгнень: ефективний моніторинг системи або мережі є важливим кроком для виявлення атак і неправильностей у системі. Він

допомагає швидко виявляти та реагувати на загрози, що може запобігти серйозним наслідкам.

10. Аудит безпеки: періодичний аудит безпеки системи або організації допомагає перевірити ефективність застосованих стратегій та заходів безпеки. Він також допомагає виявити нові загрози, які можуть виникнути з часом.

Аналіз загроз є постійним процесом, оскільки загрози постійно змінюються і еволюціонують. Важливо регулярно оцінювати та оновлювати стратегії та заходи безпеки для попередження і мінімізації загроз.

Аналіз вразливостей (vulnerability analysis) - це процес ідентифікації, оцінки та управління потенційними вразливостями інформаційно-комунікаційних систем (ІКТ).

Під час аналізу вразливостей проводяться такі кроки:

1. Ідентифікація потенційних вразливостей: це може бути виявлення вразливостей у програмному забезпеченні, налагоджених налаштувань системи, недостатньої фізичної безпеки або некоректного використання користувачами.

2. Оцінка серйозності вразливостей: на основі зібраних даних проводяться оцінка того, наскільки легко або складно може бути використання вразливості зловмисниками та як це може вплинути на функціонування системи.

3. Розробка стратегії управління вразливостями: на основі оцінки серйозності вразливостей, визначаються пріоритети по виправленню вразливостей. Також розробляються плани запобігання атак, встановлення відповідних захисних заходів та реакції на можливі атаки.

4. Виправлення вразливостей: зазвичай, відкритті вразливості вимагають внесення змін до програмного забезпечення або встановлення додаткових захисних заходів. Цей етап вимагає співпраці з розробниками програмного забезпечення та адміністраторами систем.

5. Контроль та постійний моніторинг вразливостей: після виправлення вразливостей, важливо встановити моніторингову систему, щоб вчасно виявляти та усувати нові вразливості, які можуть виникнути у майбутньому.

6. Тестування системи: після виправлення вразливостей можна провести тестування системи, щоб переконатися, що заходи безпеки дійсно працюють і не викликають конфліктів з іншими компонентами системи.

7. Оновлення і патчі: варто постійно слідкувати за оновленнями і патчами для програмного забезпечення і оперативних систем. Використання застарілих версій може стати причиною вразливостей, оскільки вони мають відомі проблеми, які вже виправлені у новіших версіях.

8. Навчання і свідомість персоналу: виробники безпеки стверджують, що найбільшим ризиком є фактор людей. Необізнані або неуважні співробітники можуть стати жертвами соціального інжинірингу, або ж можуть випадково викликати проблеми, не дотримуючись політик і процедур безпеки. Тому навчання та підвищення свідомості персоналу є важливим фактором в оптимальному управлінні вразливостями.

9. Аналіз життєвого циклу: розгляд вразливостей має бути проведений на ранніх стадіях життєвого циклу розробки системи. Це дозволяє виявити та виправити вразливості на етапі проектування та реалізації системи, що зменшує витрати та забезпечує більшу ефективність.

10. Постійне вдосконалення: аналіз вразливостей є постійним процесом, оскільки нові вразливості і методи атак постійно з’являються. Тому важливо постійно моніторити, оцінювати та виправляти вразливості, а також вдосконалювати політики та заходи безпеки.

Усі ці кроки допомагають організаціям зменшити ризик вразливостей, забезпечити адекватний рівень безпеки і захисту, а також зберегти довіру клієнтів та користувачів. Аналіз вразливостей є важливою складовою частиною цілісної стратегії безпеки ІКТ.

Аналіз вразливостей є важливим етапом в захисті інформаційних систем від зловмисних атак та витоків даних. Правильна ідентифікація та управління вразливостями допомагає забезпечити безпеку та надійність системи.

Аналіз ризиків - це процес визначення, оцінювання та керування ризиками, що можуть вплинути на досягнення мети чи успішність проекту, бізнесу або

організації. Аналіз ризиків допомагає ідентифікувати потенційні загрози та небезпеки, що можуть призвести до негативних наслідків, а також визначати можливості для використання перспективних випадків.

Процес аналізу ризиків зазвичай включає наступні кроки:

1. Ідентифікація ризиків: цей крок включає визначення всіх можливих ризиків, які можуть вплинути на проект чи бізнес, а також їх категоризацію і класифікацію.

2. Оцінка ризиків: на цьому етапі оцінюються ймовірність виникнення кожного окремого ризику та його можливий вплив на проект або бізнес. Це може бути виконано за допомогою методів, таких як аналіз попередніх випадків, експертні оцінки, статистичні дані тощо.

3. Розробка стратегій керування ризиками: після оцінки ризиків розробляються стратегії для керування ними. Це може включати прийняття заходів для запобігання виникнення ризиків, зменшення їх впливу або резервування ресурсів для реагування на випадок виникнення негативних наслідків.

4. Пріоритезація ризиків: ризики можуть мати різний рівень важливості і впливу на проект чи бізнес. Важливо визначити, які ризики потребують негайної уваги і реагування, а які можуть бути менш критичними і потребують менше уваги та ресурсів.

5. Планування запобігання ризикам: на цьому етапі розробляються конкретні заходи для запобігання виникненню ризиків. Це може включати підвищення стандартів безпеки, проведення навчань та тренінгів для працівників, встановлення контролюючих механізмів та інші заходи.

6. Розробка планів управління реагуванням на ризики: на випадок виникнення ризиків, розробляються плани дій для ефективного реагування та зменшення наслідків. Це може включати проведення додаткових досліджень, визначення резерву ресурсів, швидке прийняття рішень та інші стратегії.

7. Оцінка ефективності ризикового керування: після здійснення заходів з управління ризиками, важливо оцінити їх ефективність. Це допомагає визначити,

які стратегії були успішними, а які не дали очікуваних результатів. Оцінка ефективності дозволяє зробити корекції та вдосконалення в майбутньому.

8. Управління комунікаціями: ефективна комунікація є ключовим аспектом аналізу ризиків. Важливо побудувати механізми для обміну інформацією про ідентифіковані ризики, стратегії їх керування та зміни в планах. Це допомагає залучити всіх зацікавлених сторін, доповнює відкритість та сприяє спільному розумінню щодо ризиків і мір по їх керуванню.

Для проведення аналізу ризиків можна використати наступні методи:

1. Експертна оцінка. Цей метод використовує експертне знання та досвід фахівців для аналізу загроз. Експерти можуть бути запрошені для проведення обговорень, групових сесій чи заповнення опитувальників для збору інформації та оцінки важливості загроз.

2. SWOT-аналіз. Цей метод дозволяє виявити як сильні так і слабкі сторони організації, а також як можливості так і загрози зовнішнього середовища.

3. Матриця ризиків. Цей метод використовує матрицю для оцінки ризику на основі ймовірності та впливу загрози. Матриця допомагає визначати пріоритетність загроз і визначати необхідні заходи для їх управління.

4. Метод математичного моделювання - передбачає використання формул, алгоритмів та інших математичних інструментів для оцінки ймовірності та наслідків можливих кібератак або інших загроз інформаційній системі чи мережі. Цей підхід використовується для оцінки ризиків, пов'язаних з можливими кібератаками, витоками даних, вразливостями програмного забезпечення та іншими загрозами кібербезпеки. Методи математичного моделювання можуть бути використані для обчислення ймовірності кібератаки на основі історичних даних, обчислення вартості можливих наслідків атаки та визначення рівня ризику. Одним з популярних методів математичного моделювання є метод аналізу вартості втрати (Cost Loss Analysis - COLA). Він використовується для оцінки фінансових втрат, які можуть виникнути внаслідок кібератаки. COLA включає в себе оцінку вартості активів, імовірності атаки, вартості пошкоджень внаслідок атаки та інших факторів.

Оцінка ризиків кібербезпеки методом математичного моделювання може також включати в себе методи ризик-аналізу, такі як використання дерева подій або аналізу причин і наслідків (Fishbone діаграма). Ці методи дозволяють визначити потенційні загрози, виявити їх причини та наслідки, а також оцінити ймовірність та величину збитків.

Для проведення математичного моделювання ризиків кібербезпеки також можуть використовуватись статистичні методи, такі як ймовірність виникнення певної події на основі історичних даних. Наприклад, можна обчислити ймовірність виявлення вразливості в системі, яка може призвести до кібератаки.

У деяких випадках може бути застосована модель стохастичного процесу для прогнозування можливих кількостей кібератак протягом певного періоду часу.

Важливо пам'ятати, що математичне моделювання ризиків кібербезпеки базується на припущеннях і непередбачуваних факторах, тому результати можуть бути неповними чи не точними.

5. Бенчмаркінг. Цей метод включає порівняння діяльності організації з кращими практиками та стандартами галузі. Це дозволяє ідентифікувати можливі загрози та недоліки, а також прийняти відповідні заходи для їх усунення.

6. Аналіз PESTEL. Цей метод враховує вплив політичного, економічного, соціального, технологічного, екологічного та правового середовища на діяльність організації.

7. Аналіз трендів. Цей метод дозволяє виявити майбутні тренди та зміни в суспільстві, технології, економіці, політиці тощо, які можуть мати вплив на організацію.

Ці методи може бути використані окремо або комбіновано для отримання більш повного розуміння загроз і ризиків, що стоять перед організацією.

Використання комбінації цих методів дозволяє отримати комплексне бачення загроз і ризиків, що допоможе прийняти ефективні рішення для забезпечення безпеки та стійкості.

Методи оцінки ризиків поділяються та 3 основні типи: кількісне оцінювання, якісне оцінювання і змішане оцінювання:

1. Кількісне оцінювання ризиків: цей метод використовує точні числові дані та статистичні інформацію для розрахунку ймовірності виникнення ризиків і їх впливу на проект. Використовуються математичні моделі та статистичні методи для кількісної оцінки ризиків. Цей підхід дозволяє проводити аналіз ймовірності ризиків і визначення їх впливу на проект, шляхом розрахунку числових значень (ISAMM, RiskWatch).

2. Якісне оцінювання ризиків: цей метод базується на експертних оцінках та суб'єктивному досвіді фахівців. Використовується шкала оцінок або ранжування для визначення ймовірності і впливу ризиків. Фахівці, зазвичай, оцінюють ризики за кількома показниками, такими як імовірність виникнення, потенційний вплив, легкість виявлення тощо. Цей підхід дозволяє швидко оцінити ризики і визначити їх пріоритетність для їх зменшення або запобігання (EBIOS, OCTAVE).

3. Змішане оцінювання ризиків: цей метод поєднує кількісні та якісні елементи для оцінювання ризиків. Використовуються як числові дані, так і експертні оцінки. Наприклад, можуть використовуватися кількісні статистичні дані для розрахунку ймовірності ризику, а експертні оцінки - для визначення його впливу. Цей підхід дозволяє отримати більш комплексну і точну оцінку ризиків, враховуючи різні аспекти (CRAMM, MAGERIT).

Аналіз ризиків дозволяє зрозуміти потенційні загрози та можливості, зробити обґрунтовані рішення щодо їх керування та планування ресурсів. Це допомагає забезпечити ефективність та успішність проектів, бізнесу або організації в цілому.

Аналіз ризиків є постійним і ітеративним процесом, який потребує постійного оновлення та моніторингу. Важливо враховувати умови, які змінюються, та нові потенційні ризики, щоб забезпечити ефективний ризиковий керування і захист діяльності проекту чи бізнесу.

Аналіз ризиків є невід'ємною частиною стратегічного планування та управління. Він дозволяє організаціям попереджати та уникати можливих загроз, мінімізувати негативні наслідки та використовувати можливості для досягнення успіху. Успішний аналіз ризиків вимагає систематичного підходу, ретельного оцінювання та розробки стратегій керування для забезпечення безпеки та стабільності.

## 1.4 Аналіз методів захисту об’єктів критичної інфраструктури на основі консолідації інформації

Мета консолідації даних в аналітичних інформаційних системах полягає в об'єднанні даних з різноманітних джерел і створенні єдиного, цілісного набору даних для подальшого аналізу та аналітичної звітності. Це дозволяє організаціям отримувати зведену інформацію з різних джерел, що використовуються в різних підрозділах або філіях організації [15-16].

Консолідація даних в аналітичних інформаційних системах дозволяє:

1. Збільшити ефективність і точність аналізу. Об'єднання даних з різних джерел дозволяє отримувати повніше і більш об'єктивне уявлення про ситуацію і приймати краще обґрунтовані рішення.

2. Знизити час і зусилля, що витрачаються на пошук і збір даних. Замість того, щоб шукати інформацію в кількох системах або базах даних, з консолідованим набором даних можна отримати доступ до всієї необхідної інформації з одного місця.

3. Забезпечити єдиний стандарт для організації. Консолідація даних допомагає стандартизувати дані з різних джерел, що робить їх більш консистентними і сприяє єдності підходів до аналізу і аналітичної звітності. Це дозволяє забезпечити однаковий рівень якості і точності даних в усіх підрозділах організації.

4. Дозволяє більш ефективно використовувати ресурси. Замість того, щоб реплікувати дані в різних системах, консолідація даних дозволяє сконцентрувати інформацію в одній центрі, що дозволяє зменшити розмір і обсяг зберігання даних. Це також забезпечує більш ефективне використання обчислювальних ресурсів і зменшення накладних витрат на обслуговування і підтримку даних.

Завдання консолідації даних в аналітичних інформаційних системах включають [17-21]:

1. Ідентифікація джерел даних. Необхідно визначити всі джерела даних, з яких будуть братися дані для консолідації. Це можуть бути різні бази даних, файлові системи, зовнішні API та інші джерела.

2. Визначення структури даних. Потрібно визначити, які дані необхідно консолідувати і в якій структурі. Це включає вибір полів, таблиць і зв'язків між ними.

3. Розробка процесу консолідації. Необхідно створити процес або пайплайн для збирання даних з різних джерел і їх об'єднання в єдину базу даних або набір файлів.

4. Перевірка та очищення даних. При консолідації даних необхідно перевірити їх якість і цілісність. Це може включати видалення дублікатів, корекцію помилок і захист даних від втрати чи витоку.

5. Завершення інтеграції даних. Після консолідації даних необхідно забезпечити їх доступність для аналізу і аналітичної звітності. Це може включати розробку інтерфейсів для користувачів або сторонніх систем, які можуть працювати з цими даними.

Важливими частинами системи управління безпекою і інформацією про безпеку та події є ISMS і SIEM. Їх наявність значно покращує управління безпекою.

Інформаційна система управління безпекою (ISMS) – це система, призначена для ефективного управління безпекою інформаційних ресурсів в організації. ISMS використовує встановлені процеси, політики та процедури для захисту конфіденційності, цілісності та доступності інформації, а також для управління ризиками та забезпечення відповідності нормативним вимогам.

ISMS спирається на міжнародний стандарт ISO/IEC 27001, який визначає вимоги до створення, впровадження, оперативної підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

Однією з основних вимог до системи управління інформаційною безпекою (ISMS) є наявність процесу обробки інцидентів безпеки. Таким чином,

організаціям необхідно також запровадити і SIEM (управління інформацією про безпеку та подіями).

SIEM (Security Information and Event Management) - це комплексна система управління інформацією та подіями безпеки, яка забезпечує збір, аналіз та реагування на дані щодо безпеки з різних джерел у реальному часі.

Для створення консолідованого інформаційного ресурсу можна використовувати різні методи збору інформації, такі як ручний збір даних, автоматичне збирання даних за допомогою програмних засобів або інтеграція даних з різних джерел.

Правильна консолідація даних дозволяє організаціям отримувати більш повне і точне уявлення про свою діяльність і сприяє більш вдалим рішенням на основі об'єктивної аналітики.

### 1.5 Аналіз методів захисту інформаційних ресурсів

Аналіз методів захисту інформаційних ресурсів є важливим етапом у процесі забезпечення безпеки інформації. Це дозволяє виявити потенційні уразливості і розробити стратегії захисту, що відповідають конкретним потребам організації.

При аналізі методів захисту важливо враховувати специфіку інформаційних потреб організації та враховувати змінювані умови загроз і технологічного середовища (рисунок 1.3).

Комплексне застосування різних методів забезпечує ефективний рівень захисту інформаційних ресурсів.

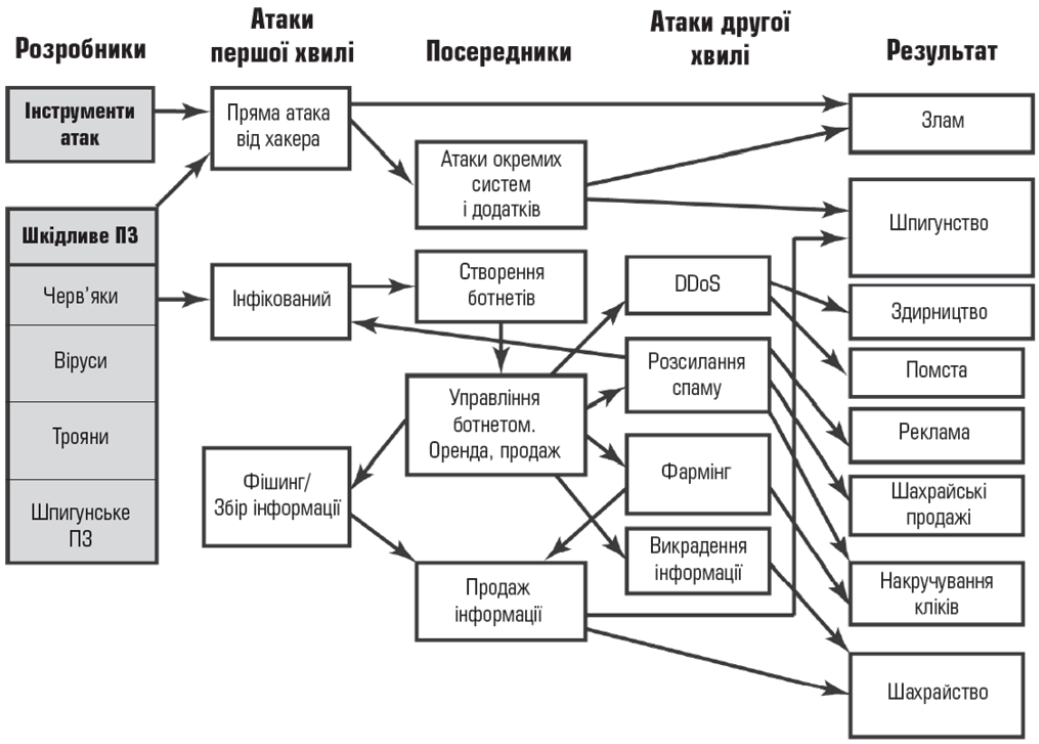



Рисунок 1.3 – Результат успішної атаки

Ось деякі з методів захисту інформаційних ресурсів:

1. Автентифікація і авторизація: установлення ідентичності користувачів і перевірка їх прав доступу до ресурсів. Це може включати введення паролів, біометричну ідентифікацію або використання токенів для доступу.

2. Шифрування: застосування алгоритмів шифрування для захисту конфіденційності даних. Шифрування може бути використане для захисту даних, які зберігаються на серверах, передаються по мережі або зберігаються на портативних пристроях.

3. Захист мережі: застосування фаєрволів і інших методів для захисту мережі від несанкціонованого доступу і атак зовні.

4. Захист проти зламу: використання програмного та апаратного забезпечення для виявлення та запобігання несанкціонованого доступу, злому та маніпуляції з інформацією.

5. Аудит і моніторинг: системи аудиту та моніторингу, що відстежують доступ до інформації та реагують на підозрілу діяльність.

6. Фізичний захист: використання захисних пристроїв, таких як контроль доступу, відеоспостереження та антикрадіжкові пристрої, для захисту фізичного доступу до інформаційних ресурсів.

7. Безпека програмного забезпечення: розробка безпечного програмного забезпечення, що використовує надійні алгоритми і практики розробки для запобігання атакам на програмне забезпечення.

8. Соціальна інженерія: освіта користувачів та тренінги для виявлення та запобігання соціальному інжинірингу, який може бути використаний для отримання несанкціонованого доступу до інформації.

9. Резервне копіювання та відновлення: Регулярна реалізація резервного копіювання даних та створення планів відновлення, які гарантують доступ до інформації у випадку аварій або катастроф.

10. Регулярні аудити та відстежування: Систематичні перевірки та аналіз рівня безпеки, а також виявлення та попередження потенційних загроз безпеці.

11. Політики безпеки: Розробка і впровадження політики безпеки, яка визначає правила, процедури та відповідальності забезпечення безпеки інформації в організації. Це може включати політики щодо паролів, використання віддалених доступів, обмеження прав користувачів тощо.

12. Пенетраційне тестування: Організація тестових атак на інфраструктуру та систему захисту для виявлення слабких місць і потенційних уразливостей. Цей метод дозволяє виявити можливі проблеми та встановити ефективні заходи щодо покращення безпеки.

13. Постійне оновлення: Регулярне впровадження оновлень і патчів для всього програмного та апаратного забезпечення, що використовується в організації. Оновлення виправляють виявлені уразливості і допомагають уникнути атак.

14. Відокремлення привілеїв: Обмеження прав доступу користувачів до критичних ресурсів. Це дозволяє уникнути несанкціонованого доступу та зменшити ризики в разі компрометації облікових записів.

15. Освіта та навчання: Проведення навчання користувачів щодо безпеки інформації, виявлення шкідливих програм та інших загроз, а також інформування про найновіші методи атак. Це допомагає залучити користувачів до захисту інформації та зменшити ризики людського фактору.

Комбінація цих методів, враховуючи конкретні потреби та характеристики організації, дозволить створити ефективну систему захисту інформаційних ресурсів. Важливо регулярно оцінювати ефективність ініційованих заходів та вносити виправлення для посилення безпеки.

### 1.6 Висновки та постановка задачі

У розділі досліджено теоретичні засади створення консолідованого інформаційного ресурсу для аналізу безпеки інформаційно-телекомунікаційної інфраструктури.

Створення консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури є кроком у напрямі поліпшення безпеки та зміцнення захисту важливої інформації. Він забезпечує доступ до цінної інформації та аналітичних інструментів, необхідних для ефективного управління ризиками та захисту від сучасних загроз.

У результаті досліджень визначились такі цілі:

- розробка архітектури ресурсу;
- розробка бази даних;
- розробка алгоритмів аналізу даних;
- висновки щодо ефективності інформаційного ресурсу.

# РОЗДІЛ ІІ. РОЗРОБЛЕННЯ ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ АНАЛІЗУ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ

## 2.1 Дослідження характеристик інформаційно-телекомунікаційної інфраструктури щодо можливості розробки консолідованого інформаційного ресурсу аналізу його безпеки

Розробка консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону має свої особливості, які варто враховувати. Деякі з них включають:

1. Збір інформації: розробка консолідованого ресурсу передбачає не лише збір безпекової інформації з різних джерел, але і необхідність її координації та інтеграції. Це дозволяє отримати комплексний огляд захищеності ІТ інфраструктури.

2. Агрегація даних: консолідований ресурс повинен мати можливість агрегувати дані з різних джерел інформації, включаючи безпекові дані, системи моніторингу, журнали подій, системи виявлення вторгнень тощо. Це дозволяє отримати повну картину безпеки ІТ інфраструктури.

3. Аналітика: консолідований ресурс має забезпечувати можливість аналізу отриманої інформації і виявлення тенденцій та вразливостей, що можуть впливати на безпеку ІТ інфраструктури.

4. Візуалізація даних: розробка такого ресурсу повинна передбачати зручний і зрозумілий інтерфейс для відображення та візуалізації даних безпеки.

5. Забезпечення конфіденційності інформації: враховування особливостей розробки системи консолідованого ресурсу має передбачати заходи збереження конфіденційності обробленої інформації та захисту її від несанкціонованого доступу.

6. Врахування регуляторних вимог: Розробка консолідованого ресурсу має враховувати вимоги законодавства щодо захисту інформації та безпеки даних, а також інших регуляторних документів, що стосуються ІТ інфраструктури регіону.

7. Співпраця зі стейкхолдерами: Розробка консолідованого ресурсу вимагає активної співпраці зі стейкхолдерами, такими як органи державного управління, оператори телекомунікаційних мереж, постачальники ІТ послуг та інші зацікавлені сторони.

8. Підтримка стандартів безпеки: Розробка консолідованого ресурсу має базуватися на визнаних стандартах безпеки, які допоможуть забезпечити однорідність і надійність аналізу безпеки.

9. Гнучкість та масштабованість: Розробка консолідованого ресурсу має бути гнучкою та легко масштабованою, щоб враховувати зміни в ІТ інфраструктурі та нові види загроз.

Врахуання цих особливостей при розробці консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону допомагають забезпечити комплексне та систематичне сприяння безпеці телекомунікаційних систем і мереж у регіоні.

Одним із ключових аспектів розробки консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону є забезпечення взаємодії та обміну даними між різними суб'єктами безпеки. Це може включати обмін інформацією з операторами телекомунікацій, лабораторіями з безпеки, органами державного управління та іншими сторонами, які мають важливу інформацію щодо безпеки ІТ інфраструктури регіону.

Також варто враховувати, що розробка консолідованого ресурсу повинна використовувати сучасні технології та інструменти для забезпечення ефективного та швидкого аналізу безпеки.

Крім того, варто забезпечити доступ до консолідованого ресурсу для відповідних структур, які займаються безпекою, та надати їм можливість аналізувати інформацію та приймати відповідні рішення щодо підвищення безпеки ІТ інфраструктури регіону.

Важливо мати відповідні процедури та політики для управління консолідованим ресурсом аналізу безпеки, включаючи забезпечення конфіденційності та захисту інформації, регулярне оновлення джерел даних та алгоритмів аналізу, а також виявлення та реагування на нові загрози та вразливості.

Загалом, розробка консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону вимагає комплексного підходу, врахування специфіки регіональної інфраструктури та взаємодії з різними стейкхолдерами. Це сприятиме ефективному контролю та підвищенню безпеки IT інфраструктури регіону.

Організація даних для розробки консолідованого інформаційного ресурсу і їх представлення передбачає кілька кроків:

1. Визначення вимог: спочатку необхідно визначити вимоги до інформаційного ресурсу. Це включає визначення потреб у даних, призначення та цільову аудиторію, а також функціональні та технічні вимоги.

2. Вибір джерел даних: далі, слід вибрати джерела даних, з яких будуть взяті дані для інформаційного ресурсу. Це може включати бази даних, файлові системи, зовнішні API, програми обліку тощо.

3. Визначення структури даних: слід визначити структуру даних, включаючи таблиці, поля та зв'язки між ними. Це відображає спосіб організації та зберігання даних у інформаційному ресурсі.

4. Розробка процесу завантаження: треба розробити процес завантаження даних. Це може включати витягування даних з джерел, трансформування та очищення їх, а також завантаження.

5. Розробка інтерфейсів: після завантаження даних, необхідно розробити інтерфейси для представлення і взаємодії з інформаційним ресурсом. Це може включати створення веб-додатків, панелей керування, аналітичних звітів та інших інтерфейсів.

6. Забезпечення безпеки: слід врахувати аспекти безпеки даних, включаючи обмеження доступу до інформації, шифрування, аудит та захист від несанкціонованого доступу.

7. Підтримка і розвиток: після запуску інформаційного ресурсу варто забезпечити постійну підтримку і розвиток системи. Це включає моніторинг та управління, виправлення помилок, розширення функціональності та оптимізацію продуктивності.

8. Визначення ключових метрик і показників: встановлення метрик і показників дозволяє вимірювати ефективність інформаційного ресурсу та об'єктивно оцінювати рівень досягнення поставлених цілей.

9. Документування процесів і змін: забезпечення докладної документації процесів та змін, які відбуваються в інформаційному ресурсі, допоможе зрозуміти логіку та контролювати внесені зміни.

10. Забезпечення якості даних: важливо забезпечити високу якість даних в, включаючи перевірку, очищення та стандартизацію даних. Це дозволить забезпечити достовірність і точність результатів аналізу.

11. Аналіз і візуалізація даних: розробка можливостей аналізу та візуалізації даних дозволяє візуально представити інформацію та дозволяє користувачам швидко здійснювати аналітичні запити і робити висновки.

12. Масштабованість і резервування даних: розробка повинна передбачати можливість масштабування і резервування даних для забезпечення стійкості та надійності системи навіть при зростанні обсягу даних або в разі відмови системи.

13. Управління доступом: забезпечення відповідного управління доступом до даних інформаційного ресурсу є важливим аспектом забезпечення конфіденційності і захисту інформації.

14. Навчання та підтримка користувачів: надання навчання та підтримки користувачам інформаційного ресурсу допоможе забезпечити ефективне використання системи та максимальне використання її можливостей.

Важливо пам'ятати, що розробка - це ітеративний процес. Під час його реалізації можуть виникати нові вимоги та потреби, які варто аналізувати і

впроваджувати для подальшого розвитку та удосконалення інформаційного ресурсу.

В цілому, розробка консолідованого інформаційного ресурсу вимагає комплексного підходу та планування, щоб забезпечити ефективне управління і доступ до цінної інформації для прийняття найкращих рішень.

## 2.2 Проектування БД консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури

Модель сутність-зв'язок (Entity-Relationship Model, ER Model) - це концептуальна модель, яка використовується для опису і проектування баз даних. Вона розглядає дані як сутності (entities), які мають атрибути (attributes) і взаємодіють між собою через зв'язки (relationships).

Основний принцип методу сутність-зв'язок полягає в ідентифікації всіх сутностей, які входять до системи, і встановленні зв'язків між ними. Сутності можуть бути фізичними об'єктами. Зв'язки ж вказують на взаємозв'язок між сутностями і можуть мати різний характер, наприклад, один-до-одного, один-до-багатьох, багато-до-багатьох.

У моделі сутність-зв'язок сутність - це об'єкт або поняття, яке може бути ідентифіковано (наприклад, критичний об’єкт). Кожна сутність має свої властивості, які називаються атрибутами (наприклад, назва об’єкту). Зв'язки визначають взаємодію між сутностями, показують, як вони пов'язані між собою.

У моделі ER зв'язки можуть мати свої властивості, які називаються атрибутами зв'язку. Вони також можуть мати ступінь, який показує кількість сутностей, що беруть участь у зв'язку (наприклад, зв'язок "багато-до-одного", "багато-до-багатьох").

Модель сутність-зв'язок також дозволяє використовувати поняття ключів, які ідентифікують унікальні екземпляри сутностей. Ключ може бути простим (один атрибут) або складним (комбінація кількох атрибутів).

Модель сутність-зв'язок є основою для проектування і розробки баз даних. Вона допомагає розібратися в структурі даних, встановити правильні зв'язки та забезпечити цілісність даних, що важливо для ефективної роботи з базою даних.

Модель сутність-зв'язок є потужним інструментом для опису структури бази даних і відношень між об'єктами в цій базі. Вона допомагає встановити правильні зв'язки між сутностями і гарантує цілісність і консистентність даних.

Для проектування консолідованого інформаційного ресурсу методом сутність-зв'язок необхідно спочатку визначити всі сутності, які входять до системи і між якими існують зв'язки. Потім визначаються атрибути, тобто властивості кожної сутності, які відображають інформацію про неї.

Після цього встановлюються зв'язки між сутностями, які можуть бути однонаправленими або двонаправленими.

Отриману модель можна використовувати для розробки бази даних, де кожна сутність стане окремою таблицею, а атрибути - стовпцями цієї таблиці. Зв'язки між сутностями відображаються за допомогою зовнішніх ключів.

Проектування консолідованого інформаційного ресурсу методом сутність-зв'язок дозволяє створити структуровану і зрозумілу модель даних, що полегшує подальше розроблення і підтримку системи.

Після моделювання структури даних за допомогою методу сутність-зв'язок, можна перейти до детальнішого проектування консолідованого інформаційного ресурсу.

Проектування консолідованого інформаційного ресурсу методом сутність-зв'язок є одним з найпоширеніших підходів до створення бази даних. Цей метод використовується для моделювання структури даних, в якій сутності представляють об'єкти, які мають важливу інформацію, а зв'язки вказують на зв'язки між цими сутностями.

Основні етапи створення ресурсу [37-42]:

- побудова ER-моделі і UML-діаграми класів;
- створення бази даних і її нормалізація;
- розробка інтерфейсу і аналітичних звітів.

Визначимо основні сутності (таблиця 2.1):

Таблиця 2.1 – Основні сутності

| | |
|---|---|
| Provider | провайдер |
| ProviderType | тип провайдера |
| OKI | об’єкт інфраструктури |
| District | район |
| Settlement | населений пункт |
| CritiCategories | категорія критичності |
| ImplLevel | рівень впровадження кіберзахисту |
| Analysis | результат аналізу безпеки об’єкту |
| User | користувач ресурсу |

Отримаємо ER-модель, яку зображену на рисунку 2.1:

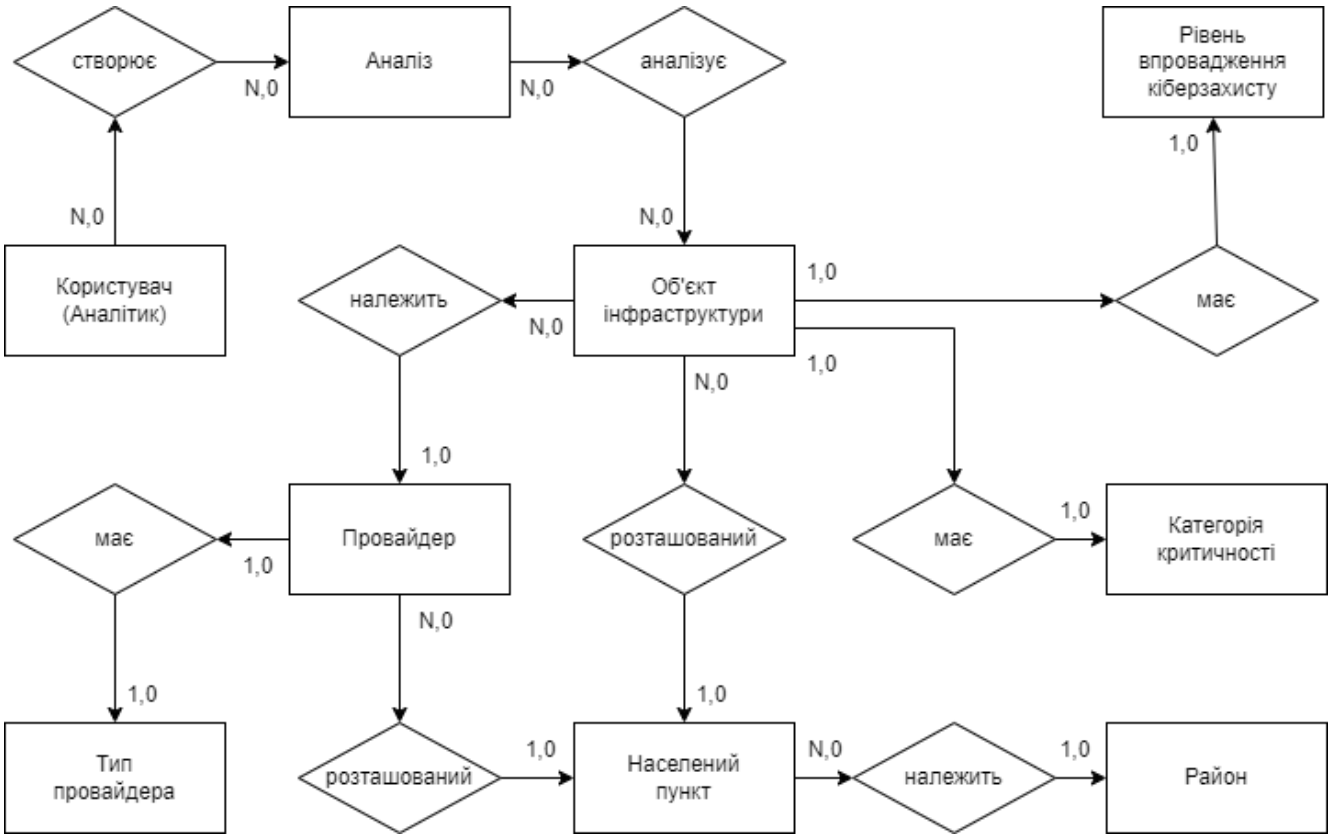



Рисунок 2.1 – ER-модель

Нормалізація бази даних - це процес організації даних у базі даних з метою зменшення дублікації і введення структурованості.

Основною метою нормалізації є уникнення аномалій бази даних, таких як втрата інформації, додаткове додавання, оновлення або видалення даних. Вона допомагає забезпечити цілісність даних, оптимізувати запити і зменшити проблеми з проектуванням та підтримкою бази даних [43-51].

Нормалізація бази даних є важливим процесом при проектуванні баз даних, оскільки вона допомагає покращити ефективність, масштабованість і цілісність даних. Крім того, нормалізована база даних буде більш гнучкою при змінах схеми або додавання нових функцій до системи.

Нормалізація бази даних зазвичай реалізується шляхом розбиття таблиць на більш малі, більш специфічні таблиці, пов'язані між собою за допомогою зв'язків. Цей процес грунтується на наборі правил, відомих як нормальні форми.

У загальному випадку, існує п'ять нормальних форм, які описують рівні нормалізації бази даних. Це:

1. Перша нормальна форма (1NF): Дані мають бути розбиті на недільниківі атомарні значення.

2. Друга нормальна форма (2NF): Всі атрибути (стовпці) в таблиці повинні пов'язуватися з первинним ключем і не залежати один від одного.

3. Третя нормальна форма (3NF): Всі неключові атрибути повинні залежати від первинного ключа без залежностей між атрибутами.

4. Четверта нормальна форма (4NF): Залежності між неключовими атрибутами ізолюються в окремі таблиці.

5. П'ята нормальна форма (5NF): Моделювання декомпозиції даних до досягнення чистого вигляду, де всі залежності вже залежать від первинного ключа.

Нормалізація бази даних дозволяє досягти ефективнішої роботи з даними, підвищити продуктивність та зменшити ризик втрати або некоректного використання даних. Однак, важливо знати, що глибока нормалізація може

призвести до складних запитів при отриманні даних з бази. Тому, потрібно збалансувати між нормалізацією та простотою використання бази даних.

Нормалізація бази даних може бути виконана за допомогою декількох кроків:

1. Ідентифікація сутностей: Спочатку потрібно ідентифікувати сутності (об'єкти), які потрібно зберігати в базі даних.

2. Визначення атрибутів: Для кожної сутності потрібно визначити атрибути (властивості), які описують цю сутність.

3. Визначення первинного ключа: Потрібно визначити первинний ключ, який є унікальним і однозначно ідентифікує кожен запис у таблиці.

4. Розбиття на таблиці: Потрібно розбити сутності на більш малі таблиці, які мають мінімальну дублікацію даних. Цей процес називається декомпозицією.

5. Встановлення зв'язків: Потрібно встановити зв'язки між необхідними таблицями за допомогою зовнішніх ключів. Це дозволяє забезпечити цілісність даних і запобігає втраті зв'язаної інформації.

6. Перевірка нормальних форм: На кожному етапі декомпозиції потрібно перевіряти, чи відповідають таблиці нормальній формі. Якщо таблиця не відповідає вимогам нормальної форми, можуть бути потрібні додаткові зміни для досягнення нормалізації.

По завершенню процесу нормалізації отримаємо таку UML-діаграму класів (мал.2.2):

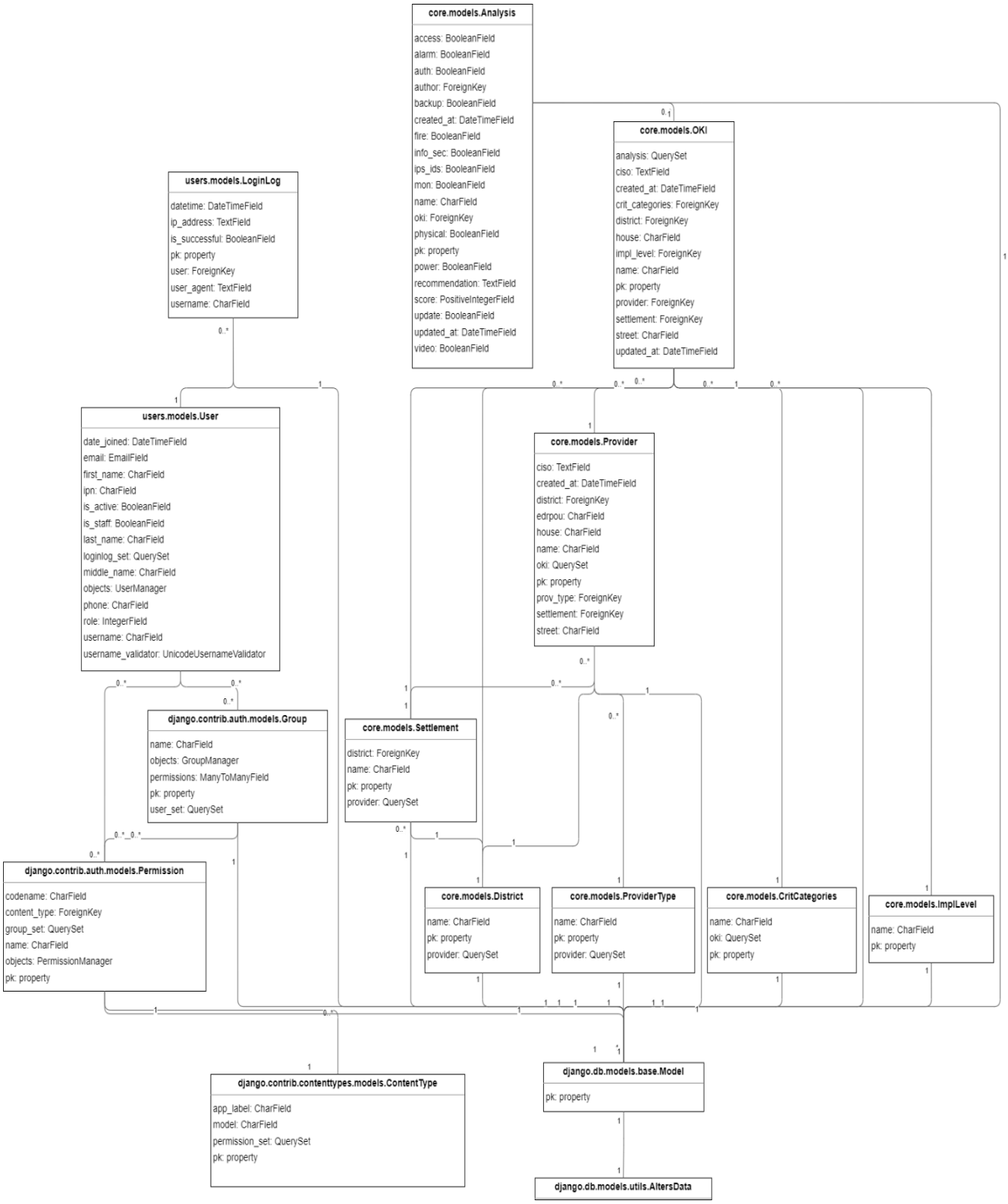



Рисунок 2.2 – UML діаграма класів

## 2.3 Захист розробленого консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури

Для забезпечення безпеки ресурсу налаштуємо ті види захистів, який надає веб-фреймворк Django і додатково посилимо розробленим захистом.

Фреймворк Django забезпечує різноманітні види захисту для веб-додатків:

1. Захист від кросс-сайтового скриптінгу (XSS): Django автоматично екранує дані, що вводяться користувачами, перед їхнім відображенням на веб-сторінках. Це запобігає виконанню шкідливого JavaScript на сторінках і захищає від атак XSS.

2. Захист від крадіжки сесій (session hijacking): Django генерує та керує унікальними сесійними ідентифікаторами для кожного користувача. Це дозволяє унікально ідентифікувати користувачів і забезпечує безпеку сесій.

3. Захист від крадіжки і підробки запитів (CSRF): Django автоматично додає унікальні токени до форм на сторінках, які дозволяють перевірити, що запити надіслані з правильного джерела. Це запобігає атакам CSRF, які можуть використовувати підроблені запити.

4. Захист від SQL-ін'єкцій: Django надає інструменти, щоб уникнути SQL-ін'єкцій, завдяки використанню параметризованих запитів і санітаризації вхідних даних.

5. Захист від перенаправлення Open Redirect: Django має вбудований захист від атак перенаправлення Open Redirect, що дозволяє контролювати, куди перенаправляється користувач після аутентифікації.

6. Захист від переповнення буфера: Django автоматично перевіряє та обробляє вхідні дані, щоб уникнути переповнення буфера та інших подібних атак.

7. Захист від витоку інформації: Django забезпечує захист конфіденційної інформації шляхом шифрування паролів, сесійних даних та інших чутливих даних на сервері та під час передачі через мережу.

8. Захист від небезпечних завантажень: Django дозволяє налаштовувати обмеження на типи файлів, які можуть бути завантажені від користувачів, тим самим запобігаючи завантаженню шкідливого коду або вразливих файлів.

9. Захист від атак на схему URL: Django має можливості для врегулювання атак від краще відомого як "Directory traversal" або "path traversal".

10. Захист від небезпечних запитів: Django має можливості для виявлення та блокування небезпечних запитів, таких як запити зі зламаними параметрами.

11. Обмеження дозволених хостів (ALLOWED_HOSTS), які можуть використовувати ваш Django додаток. В цьому списку можна задати конкретні домени або шаблони доменів, які ви довіряєте.

12. Автентифікація та авторизація: Django має вбудовану систему користувачів, яка дозволяє аутентифікувати і авторизувати користувачів. Вона надає засоби для створення системи ролей та дозволів.

13. Вбудований механізм логування: Django дозволяє реєструвати та контролювати події в системі, що дозволяє своєчасно отримувати інформацію для виявлення і запобігання будь-яким потенційним атакам.

14. Перевірка прав доступу: Django надає механізми для визначення та керування правами доступу до різних частин веб-додатків. Це дозволяє обмежити доступ користувачів до конфіденційної інформації та функціональності.

15. Перевірка безпеки сторонніх бібліотек: Django має інструменти для перевірки безпеки сторонніх бібліотек, які використовуються у веб-додатку, що допомагає уникнути використання вразливих версій або бібліотек з відомими проблемами безпеки.

Для підвищення безпеки інформаційного ресурсу створено додатковий захист:

1. Двофакторна автентифікація, яка складається із пари «Логін/пароль» і «Одноразовий пароль TOTP (Time-based One-Time Password)» на основі часу - відбувається шляхом введення логіна і пароля з підтвердженням тимчасового одноразового коду двофакторної автентифікації.
2. Шлях входу на сайт визначається в залежності від ролі користувача;

3. Доступи до певних таблиць даних в залежності від ролі користувача;
4. Журнал спроб входу із збереженням IP-адрес.

## 2.4 Висновки до розділу

Наявність захищеної інформаційно-телекомунікаційної інфраструктури є критично важливою для розвитку сучасного суспільства і економіки.

Інформаційно-телекомунікаційна інфраструктура грає важливу роль у комунікації між людьми, організаціями і країнами, тому розвиток інформаційно-телекомунікаційної інфраструктури є критично важливим для сучасного суспільства. Вона допомагає вирішувати глобальні проблеми, стимулює економічне зростання та сприяє розвитку людей.

Інформаційно-телекомунікаційна інфраструктура є важливою для надання послуг зв’язку і інтернет. У той же час, безпека інформаційно-телекомунікаційної інфраструктури піддається різного роду загрозам і ризикам, які можуть вплинути на її стабільність та надійність.

У даному розділі було визначено основні сутності і спроектовано базу даних,.

Розглянуті і налаштовані захисти, які надає фреймворк Django, а також, безпеку ресурсу було посилено розробленим додатковим захистом.

# РОЗДІЛ ІІІ. РОЗРОБЛЕННЯ ПРОГРАМИ СИСТЕМНОГО АНАЛІЗУ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ СТВОРЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ

## 3.1 Обґрунтування вибору СУБД та мови програмування

Існує кілька основних причин, чому PostgreSQL може бути обраним як СУБД для проекту.

1. Відкритий і безкоштовний: PostgreSQL є вільним і відкритим програмним забезпеченням, що дозволяє його безкоштовне використання для розробки проекту. Він не вимагає придбання ліцензій і забезпечує доступ до вихідного коду, що дозволяє змінювати програмне забезпечення під свої потреби.

2. Масштабованість і продуктивність: PostgreSQL може працювати з великими обсягами даних і високої навантаження на сервер. Він має оптимізовану систему кешування, яка поліпшує продуктивність запитів. Також PostgreSQL підтримує горизонтальне масштабування, що дозволяє розподіляти навантаження на кілька серверів.

3. Розширюваність: PostgreSQL дозволяє розширювати свої можливості шляхом створення власних функцій, типів даних та інших розширень. Він має розвинутий інтерфейс для програмування на мовах, таких як C, Python, Java і багатьох інших.

4. Безпека: PostgreSQL забезпечує широкий набір заходів безпеки, таких як автентифікація, ролева базова система доступу і шифрування даних. PostgreSQL також має вбудовану підтримку SSL-шифрування для захисту даних під час передачі.

5. Гнучкість: PostgreSQL має велику кількість вбудованих функцій, що дозволяє виконувати складні операції з даними. Він має підтримку географічних і геометричних типів даних, повнотекстового пошуку, роботи з JSON і багатьох

інших технологій. PostgreSQL також підтримує розширення SQL-стандарту і має широкий набір додаткових модулів.

6. Підтримка ACID властивостей: PostgreSQL гарантує виконання ACID принципів (Atomicity, Consistency, Isolation, Durability). Це означає, що воно забезпечує надійне зберігання і цілісність даних, а також, здатність до відновлення після відмови системи.

7. Супроводження та підтримка спільноти: PostgreSQL має велику та активну спільноту користувачів та розробників, яка надає не тільки технічну підтримку, але й регулярно оновлює та розширює можливості СУБД. Також існує комерційна підтримка PostgreSQL, яка дозволяє отримати додаткову допомогу та консультування.

8. Сумісність з іншими базами даних: PostgreSQL підтримує стандарти SQL і ANSI, що дозволяє зручно переносити існуючий код і додатки з інших баз даних. Також PostgreSQL має можливість підключати зовнішні розширення та модулі, що полегшує інтеграцію з іншими системами.

9. Широкий набір інструментів і бібліотек: PostgreSQL має багато розширень, інструментів та бібліотек, які спрощують розробку і підтримку проекту. Наприклад, існують різні графічні інтерфейси для адміністрування баз даних, ORM-фреймворки, засоби для моніторингу та налагодження запитів, і багато іншого.

10. Довгий термін підтримки: PostgreSQL має довгий термін підтримки (мінімум 5 років) для кожної версії. Це дає можливість мати стабільну і безпечну систему управління базами даних, яка регулярно отримує оновлення, а патчі та зміни налагоджуються.

11. Реплікація і висока надійність: PostgreSQL надає можливості реплікації, що дозволяє створювати резервні копії даних або створювати стендбай-сервери для забезпечення неперервної роботи системи. Реплікація в PostgreSQL може бути реалізована за допомогою логічного або фізичного рівнів реплікації.

12. Індексація та оптимізація запитів: PostgreSQL має розширену систему індексів, яка дозволяє покращити продуктивність запитів. Вона підтримує багато

видів індексів, включаючи B-tree, hash, GiST та GIN, що дозволяє оптимізувати запити для різних сценаріїв.

13. Підтримка стандартів: PostgreSQL дотримується багатьох SQL-стандартів, що дозволяє вам легко мігрувати ваші дані до і з інших СУБД. Він також підтримує інші стандарти, такі як JSON, XML, GIS, що робить його універсальним інструментом для роботи з різними типами даних.

14. Підтримка геоданих: PostgreSQL має вбудовану підтримку роботи з геоданими і геопросторовими запитами. Він надає можливості для зберігання, індексування та обробки геоданих, що робить його ідеальним вибором для проектів, пов'язаних з географією та картографією.

15. Хмарна сумісність: PostgreSQL підтримується багатьма провайдерами хмарних послуг, такими як Google Cloud Platform (GCP), Microsoft Azure, Amazon Web Services (AWS). Це дозволяє легко розгорнути та масштабувати базу даних PostgreSQL в хмарному середовищі.

16. Загальноприйняте використання: PostgreSQL вважається однією з найпопулярніших СУБД, що використовуються у світі. Він має велику спільноту користувачів та розробників, активні форуми та ресурси для обміну досвідом та розв'язання проблем. Використання PostgreSQL дозволяє залучити в проект кваліфікованих фахівців, а також з легкістю знайти відповіді на відкриті питання та проблеми.

Загалом, PostgreSQL є потужною, розширюваною, безпечною і надійною СУБД, яка може задовольнити потреби будь-якого проекту. Вважаючи всі ці переваги, обрання PostgreSQL - розумний вибір для будь-якого проекту, який потребує надійного та ефективного зберігання та обробки даних.

Враховуючи всі перелічені фактори, можна прийти до висновку, що PostgreSQL є привабливим вибором для проектів будь-якої масштабності та складності. Його надійність, продуктивність, безпека, розширюваність і підтримка забезпечують ефективну роботу з базою даних та задоволення потреб проекту.

Ці чинники роблять PostgreSQL привабливим вибором для проекту, що потребує масштабованого, продуктивного, безпечного та гнучкого управління базами даних.

Розглянемо поєднання мови програмування Python із web-фреймворком Django для розробки консолідованого інформаційного ресурсу.

Мова програмування Python вважається однією з найпопулярніших та універсальних мов програмування. Ось кілька причин, чому Python є відмінним вибором для розробки програмного забезпечення:

1. Простота вивчення: Python має простий і легкий для розуміння синтаксис. Це дозволяє навчитися програмуванню швидко і ефективно, що особливо важливо для початківців.

2. Велика спільнота розробників: Python має активну спільноту розробників, яка постійно поповнюється новими бібліотеками та фреймворками. Це робить мову багатогранною і гнучкою для різних застосувань.

3. Кросплатформеність: Python підтримується на більшості операційних систем, включаючи Windows, macOS та Linux. Це означає, що програми, написані на Python, можуть працювати на різних пристроях без необхідності переписування коду.

4. Багата бібліотека: Python має велику кількість бібліотек та фреймворків, що спрощують розробку програмного забезпечення. Наприклад, бібліотека NumPy дозволяє працювати з багатовимірними масивами та математичними функціями, а фреймворк Django допомагає розробляти веб-додатки.

5. Широкі можливості: Python використовується в різних сферах, включаючи веб-розробку, наукові дослідження, машинне навчання, аналіз даних та багато іншого. Це дозволяє розробникам займатися різноманітними проектами і розширити свої навички.

Узагалі, Python є потужною та ефективною мовою програмування, яка має чимало переваг для розробників будь-якого рівня. Він поєднує в собі простоту вивчення з широкими можливостями та сприяє швидкому розвитку програмного забезпечення.

Ще однією вагомою перевагою Python є його висока читабельність. Синтаксис мови відповідає природній мові, що робить код зрозумілим і легко читабельним для інших розробників. Це особливо важливо в командних проектах, де різні розробники співпрацюють над одним кодом.

Python також володіє багатим екосистемою, яка дозволяє швидко розробляти програмне забезпечення. У мові вже є велика кількість бібліотек та модулів для різних завдань, що дозволяє скоротити час розробки. Наприклад, бібліотека Pandas дозволяє легко та швидко працювати з даними, а бібліотека Matplotlib допомагає візуалізувати дані.

Python також відомий своєю підтримкою штучного інтелекту. Такі популярні бібліотеки як PyTorch та TensorFlow роблять розробку моделей машинного навчання більш доступною і простою для розробників. Таким чином, Python є популярним вибором для реалізації проектів інтелектуального аналізу даних.

Крім того, Python – це мова з відкритим кодом, що означає, що ви можете змінювати та розповсюджувати його безкоштовно. Тому Python доступний для широкого кола розробників та сприяє швидкому розвитку мови завдяки активному співробітництву та постійним оновленням.

Враховуючи всі ці переваги, Python стає першим вибором для багатьох розробників. Він поєднує легкість вивчення з потужною функціональністю, що робить його надійним варіантом для розробки програмного забезпечення будь-якого рівня складності.

Додатковою перевагою мови програмування Python є велика кількість ресурсів для навчання та підтримки. Існує безліч онлайн-курсів, підручників, форумів та спільнот, в яких можна знайти відповіді на питання, отримати допомогу та ділитися досвідом з іншими розробниками. Це дозволяє ефективно вивчити мову та швидко знайти відповіді на проблеми, які можуть виникнути під час розробки.

Python також володіє широкими можливостями інтеграції з іншими мовами програмування. Наприклад, ви можете використовувати C/C++ код у ваших

програмах на Python, що дозволяє покращити швидкодію та розширити функціональність вашого програмного забезпечення.

Python також підтримує розробку веб-додатків завдяки популярним фреймворкам, таким як Django та Flask. Ці фреймворки спрощують роботу з веб-технологіями та допомагають швидко створювати потужні та масштабовані веб-додатки.

Крім того, Python є мовою, яка поєднує скриптову та об'єктно-орієнтовану парадигми програмування. Це робить його дуже гнучкою і потужною для розробки різноманітних проектів. Ви можете використовувати Python для написання коротких скриптів або створення великих та складних систем.

Отже, з урахуванням всіх цих факторів, вибір мови програмування Python стає логічним і ефективним для багатьох розробників. Вона поєднує простоту, гнучкість, широкі можливості та має велику спільноту підтримки, що робить її ідеальним вибором для будь-якого проекту розробки програмного забезпечення.

Вибір web-фреймворка Django для розробки консолідованого інформаційного ресурсу має кілька переваг:

1. Швидкість розробки: Django надає потужний інструментарій для розробки, що дозволяє розробникам швидко створювати функціональні веб-додатки. Django забезпечує автоматичне адміністрування та ряд інших стандартних функціональних можливостей, що допомагають зосередитись на основних завданнях розробки.

2. Масштабованість: Django розроблений для роботи з великими проектами і має вбудовану підтримку для масштабованості. За допомогою вбудованого модуля ORM Django можна працювати з базами даних різних типів, таких як PostgreSQL, MySQL, SQLite і багатьох інших. Крім того, Django надає можливості для кешування, розподіленого кешування, розподіленої обробки та багато інших механізмів для оптимізації продуктивності.

3. Безпека: Django має вбудовану підтримку забезпечення безпеки. Він надає захист від багатьох типів атак, таких як XSS (cross-site scripting), CSRF (cross-site request forgery) тощо. Django також має вбудовану підтримку аутентифікації і

авторизації, яка дозволяє розробникам легко управляти доступом користувачів до ресурсів.

4. Гнучкість: Django дає розробникам велику гнучкість при створенні власного веб-додатку. Він не накладає жорстких обмежень на архітектуру або організацію коду, що дозволяє розробникам використовувати власні рішення та підходи до розробки.

5. Велика спільнота: Django є одним з найпопулярніших web-фреймворків, і має велику активну спільноту розробників. Це означає, що завжди є наявні ресурси та документація для отримання допомоги, а також безліч сторонніх пакетів і розширень, які допоможуть прискорити розробку із використанням Django.

6. Висока якість коду: Django пропонує стандартизований підхід до розробки і підтримує високу якість коду. Він сприяє розподіленню функціоналу по різних модулях, що допомагає зробити код більш організованим, читабельним і легко зрозумілим.

7. Вбудована адміністративна панель: Django надає вбудовану адміністративну панель, яка дозволяє легко створювати і змінювати дані, а також керувати правами доступу користувачів. Це дуже зручно для консолідованого інформаційного ресурсу, якщо потрібно проводити оновлення та відслідковувати зміни великої кількості даних.

8. Підтримка веб-сервісів: Django має вбудовану підтримку роботи з веб-сервісами, що дозволяє легко взаємодіяти з іншими системами через REST або SOAP протоколи. Це дозволяє розробляти консолідований інформаційний ресурс з можливістю обміну даними з іншими ресурсами.

9. Підтримка міжнародних проектів: Django пропонує вбудовану підтримку локалізації і мультимовності, що робить його ідеальним вибором для розробки консолідованого інформаційного ресурсу, який має багатомовний інтерфейс і працює з різними культурами та локалізованими даними.

10. Відкритий код: Django є проектом з відкритим вихідним кодом. Це означає, що розробники можуть використовувати його безкоштовно, а також

вносити внески в розвиток фреймворку. Опен-сорс модель також сприяє активній спільноті, яка постійно випускає нові оновлення, плагіни й розширення для покращення роботи Django.

11. Оптимальна робота з базами даних: Django має вбудовану ORM (Object-Relational Mapping), що дозволяє легко працювати з реляційними базами даних. ORM спрощує взаємодію з базою даних, забезпечує безпеку і запобігає SQL-injection атакам. Крім того, Django підтримує міграції даних, що дозволяє легко змінювати схему бази даних без втрати даних.

12. Розширюваність: Django має модульну структуру і пропонує систему плагінів, що дозволяє розширювати його функціональність і додавати нові можливості до проекту. Це забезпечує гнучкість і можливість адаптувати фреймворк під потреби розробки консолідованого інформаційного ресурсу.

13. Хороша документація: Django має дуже добре викладену документацію, яка охоплює всі основні аспекти розробки. Це дає можливість швидко вивчити фреймворк і розпочати розробку без зайвих запитань і труднощів.

14. Сумісність з іншими технологіями: Django може легко взаємодіяти з іншими технологіями, такими як JavaScript фреймворки (наприклад, React або Angular), різні сервіси API, веб-сервери (наприклад, Nginx або Apache) тощо. Це дозволяє побудувати комплексний інформаційний ресурс з використанням різних інструментів і технологій.

15. Підтримка безперервної інтеграції та розгортання: Django має усі необхідні інструменти та підходи для налаштування процесу безперервної інтеграції та розгортання (CI/CD). Це дозволяє автоматизувати процеси тестування, зборки і розгортання додатку, що зменшує ризик помилок та полегшує процес розробки та випуску оновлень.

16. Розширені можливості управління змінами: Django має вбудовану систему контролю версій, яка дозволяє відстежувати та керувати змінами в коді проекту. Це особливо корисно при колективній розробці або при роботі над великими проектами зі складною ієрархією коду.

17. Підтримка SEO: В Django враховано багато SEO-принципів та оптимізацій. Через правильну організацію URL-адрес, генерацію мета-тегів, роботу із заголовками сторінок та інші оптимізаційні можливості, Django допомагає покращити видимість вашого ресурсу у пошукових системах.

18. Висока надійність: Django має вбудовану обробку помилок і винятків, автоматичне відновлення після збоїв та резервне копіювання даних. Це гарантує безперебійну роботу ресурсу та запобігає втратам інформації.

19. Багатомодульність: Django легко інтегрується з різними модулями і бібліотеками як для функціональних, так і для дизайнерських можливостей. Це дає змогу розширювати можливості ресурсу залежно від потреб проекту.

20. Простота міграції до нових версій: Django має добре продуману систему міграцій, що полегшує процес переходу на нові версії фреймворку без необхідності переписування вже існуючого коду. Це дозволяє забезпечувати актуальність свого ресурсу та отримувати нові функціональність без великих зусиль.

Ці переваги спільно дозволяють Django стати потужним і ефективним інструментом для розробки консолідованого інформаційного ресурсу, забезпечуючи швидкість, безпеку, масштабованість та гнучкість, необхідні для успішного виконання проекту.

## 3.2 Програмна реалізація створеного консолідованого інформаційного ресурсу

Однією з найпотужніших функцій Django є ORM (Object-Relational Mapping) - об’єктно-реляційне відображення, яке дає змогу взаємодіяти з базою даних, як із SQL. Це просто пітонічний спосіб створення SQL для запитів і маніпулювання базою даних, а також, отримання результатів пітонічним способом. Це лише спосіб, але це дуже розумна інженерія, яка використовує переваги деяких складніших частин Python.

Для роботи з базою даних Django використовує систему Django-моделей.

Django-модель - це клас, який визначає структуру та поведінку даних в базі даних. Вона використовується в фреймворку Django для взаємодії з базою даних, забезпечуючи доступ до даних, збереження та модифікацію. Кожна Django-модель представляє окрему таблицю в базі даних і містить атрибути-поля, які визначають типи даних та обмеження для кожного поля. Django-модель також має методи, які дозволяють проводити операції з даними, такі як пошук, сортування та фільтрацію.

Це надає можливість використовувати автоматично створений API для доступу до необхідних даних бази даних.

Практична реалізація бази даних на Django може включати кілька кроків:

1. Визначення моделей: у файлі `models.py` кожного оголошеного додатку визначаються моделі, які необхідно використати у базі даних. Наприклад, модель `User`, можна створити як клас, що наслідується від `django.db.models.Model` і містить потрібні поля.

2. Створення міграцій: після визначення моделі, необхідно згенерувати файли міграцій, які містять код SQL для створення таблиць бази даних і допомагає утримувати базу даних у актуальному стані.

3. Виконання міграцій: на основі створених міграцій необхідно запустити процес створення таблиць бази даних.

4. Взаємодія з базою даних: тепер можна взаємодіяти з базою даних за допомогою Django ORM.

5. Відображення даних: використовуючи шаблони та представлення Django, можна відображати дані з бази даних у веб-додатку.

Це основні кроки для реалізації бази даних на Django. Звичайно, є багато деталей і додаткових можливостей, які можна налаштувати та використовувати, але це надає загальну уяву про структуру та процес створення бази даних на Django.

В результаті, отримані такі основні таблиці (таблиця 2.2):

Таблиця 2.2 – Отримані основні таблиці бази даних

| | |
|---|---|
| Provider | дані провайдерів |
| ProviderType | довідник типів провайдерів |
| OKI | дані об’єктів інфраструктури |
| District | довідник районів |
| Settlement | довідник населених пунктів |
| CritiCategories | довідник категорій критичності |
| ImplLevel | довідник рівнів впровадження кіберзахисту |
| Analysis | результати аналізів безпеки об’єкту |
| User | користувачі системи |
| LoginLog | журнал спроб входу |
| AdminLog | журнал дій користувачів |
| TotpDevice | пристрої 2FA |

Після отримання ER-моделі і UML-діаграми класів, створені таблиці бази даних.

На рис.3.1-3.2 представлена схема бази даних:

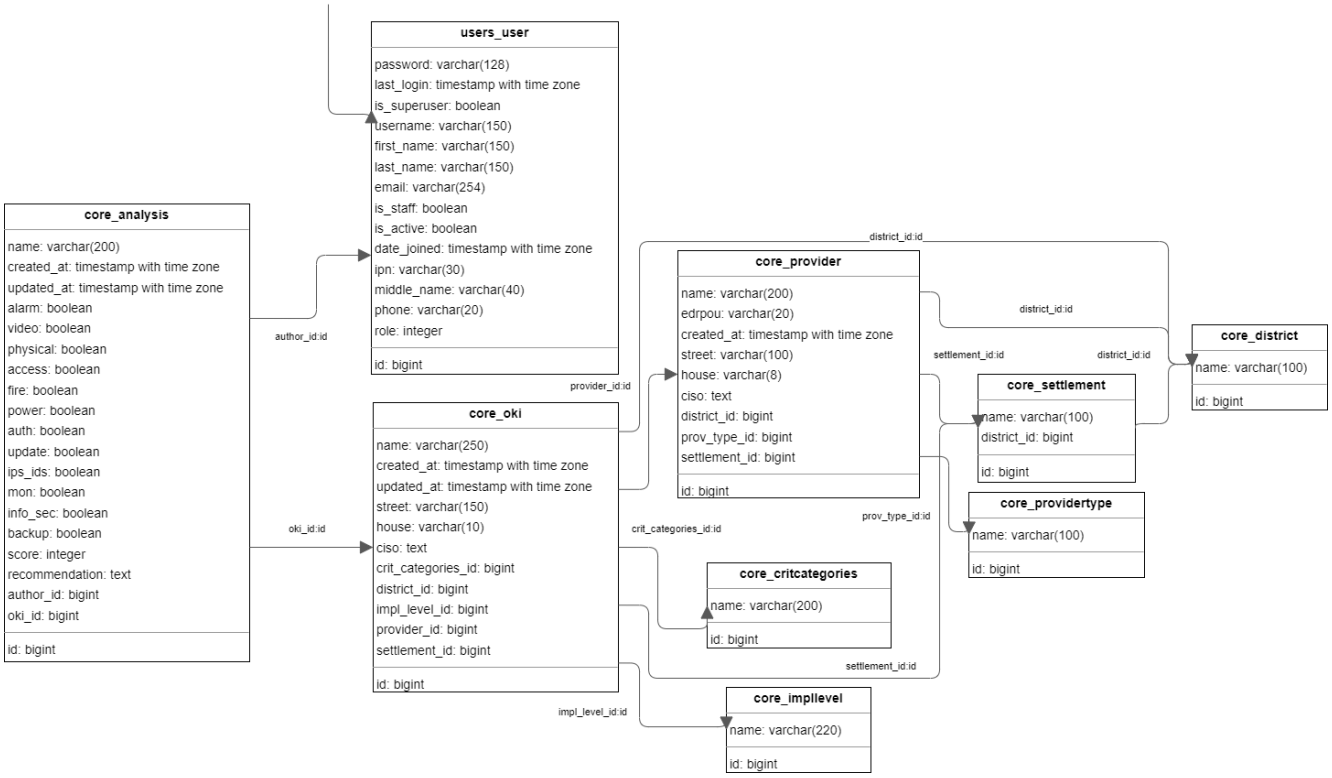



Рисунок 3.1 – Схема бази даних, частина 1

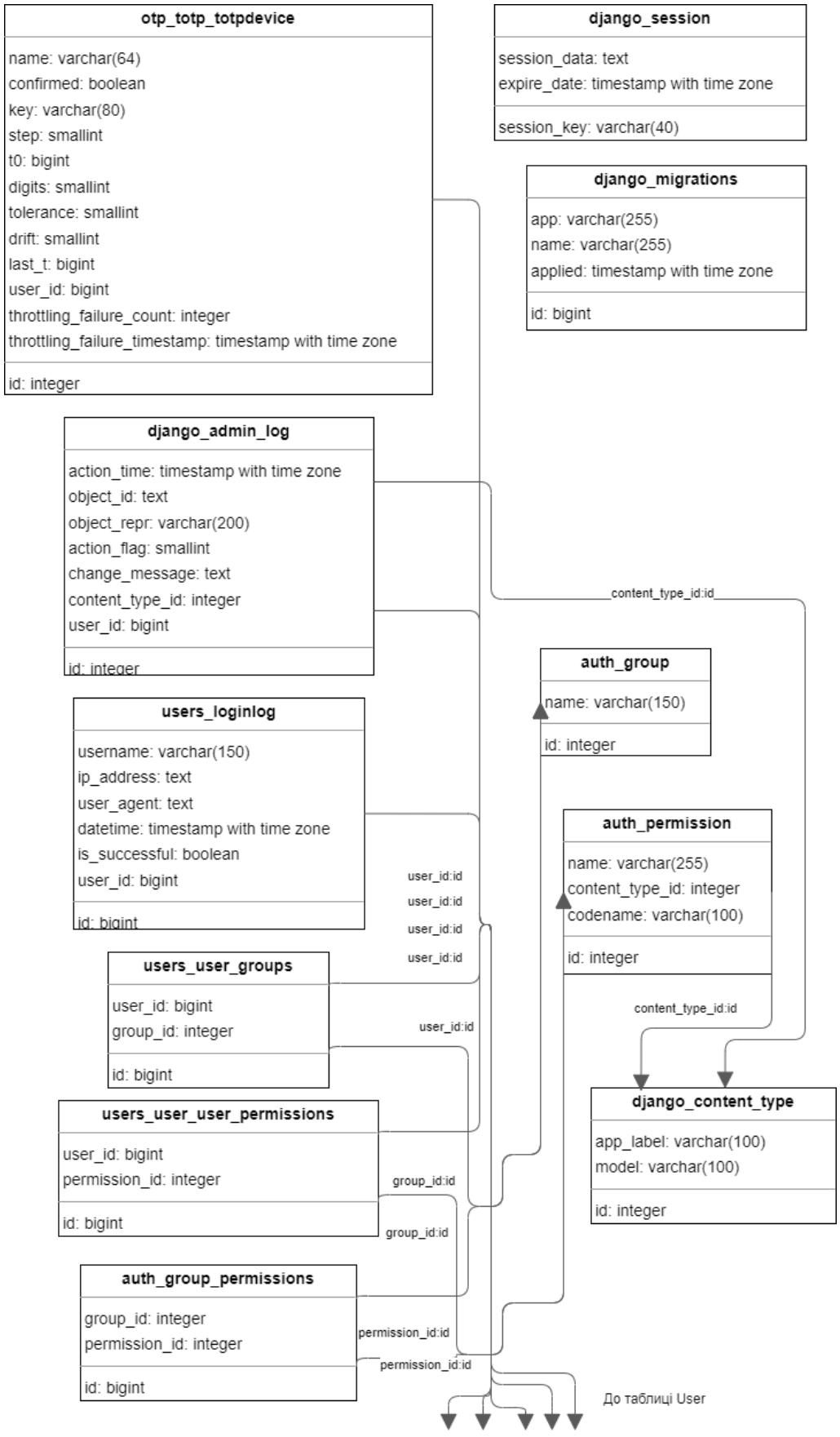



Рисунок 3.2 – Схема бази даних, частина 2

## 3.3 Програмна реалізація модулів захисту консолідованого інформаційного ресурсу

Захист інформаційного ресурсу є одним з найважливіших завдань для будь-якої організації, оскільки конфіденційність, цілісність і доступність даних є критично важливими аспектами, які необхідно забезпечити.

Розробка програмних модулів забезпечення захисту інформаційного ресурсу передбачає вивчення всіх можливих векторів атак, слабкі місця системи та ризики, що можуть вплинути на безпеку.

Після визначення потенційних загроз та ризиків, наступним етапом є розробка програмного модуля забезпечення захисту інформаційного ресурсу.

Це може включати реалізацію механізмів аутентифікації, авторизації, шифрування, контролю доступу та інших захисних механізмів.

Розробка програмних модулів забезпечення захисту інформаційного ресурсу є постійним процесом, оскільки загрози безпеці постійно змінюються і розвиваються. Тому важливо постійно оновлювати та покращувати захисні механізми, щоб забезпечити максимальну безпеку інформаційного ресурсу.

Розробка таких модулів є складним процесом, що вимагає глибоких знань у сфері кібербезпеки. Вона передбачає аналіз загроз і ризиків, розробку стратегії захисту, реалізацію механізмів безпеки, моніторинг та аудит безпеки, контроль доступу і тестування на проникнення. Результатом цієї роботи є створення безпечного інформаційного ресурсу, що забезпечує конфіденційність, цілісність і доступність даних.

Застосування контролю доступу є теж одним із способів забезпечення безпеки інформаційного ресурсу і включає встановлення правил та обмежень доступу до різних частин системи для різних користувачів - надання дозволів користувачу на доступ до окремих таблиць згідно його ролі або членства в групі. Також, можливе і індивідуальне налаштування дозволів.

Важлива інформація буде доступна тільки обмеженому колу осіб з високими привілеями, тоді як звичайним користувачам можуть бути надані обмежені права доступу.

Розроблений журнал спроб входу, який надає адміністратору можливість відстежувати коли і чи успішно відвідувач зміг зайти на сайт як користувач.

В процесі розробки налаштовано всі види захистів, які надає веб-фреймворк Django, а також, розроблено додаткові захисти:

- двофакторна автентифікація;
- контроль доступу користувачів;
- окремий шлях входу на сайт в залежності від ролі користувача;
- журналювання спроб входу.

## 3.4 Розробка програми системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону на основі створеного інформаційного ресурсу

Зайдемо на сайт для проведення аудиту об’єктів критичної інфраструктури і отримання його результатів.

У зв’язку з підключенням двофакторної автентифікації, процедура входу на сайт складається з двох етапів:

1. Введення логіна і пароля.
2. Введення одноразового тимчасового коду.

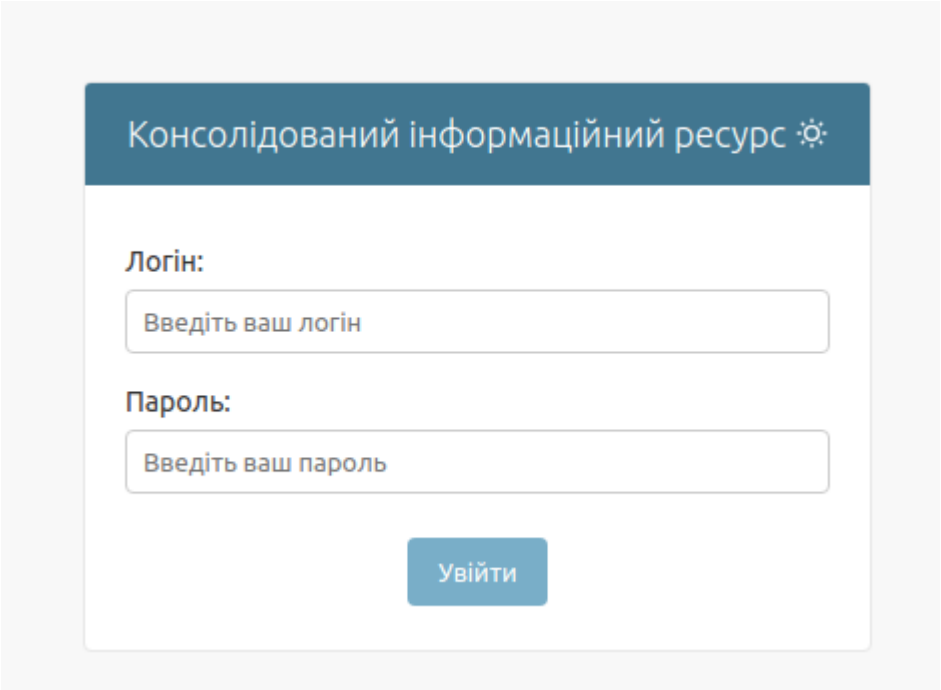



Рисунок 3.3 – Ведення логіна і пароля

Якщо користувач заходить на сайт вперше, йому необхідно налаштувати пристрій 2FA, при подальших входах проводити налаштування не потрібно.

Адміністратор має можливість видалити цей пристрій 2FA, якщо користувач його втратив, після чого, користувач заходить як вперше і створює новий 2FA - пристрій.

Після проходження процедури автентифікації користувача буде перенаправлено на сторінку кабінету згідно його ролі.

На рисунку 3.4 показано форму, за якою здійснюється введення інформації про стан захищеності об’єкту. Всього наявно 10 питань, з яких 5 питань по стану фізичного захисту і 5 питань по стану кібербезпеки об’єкту.

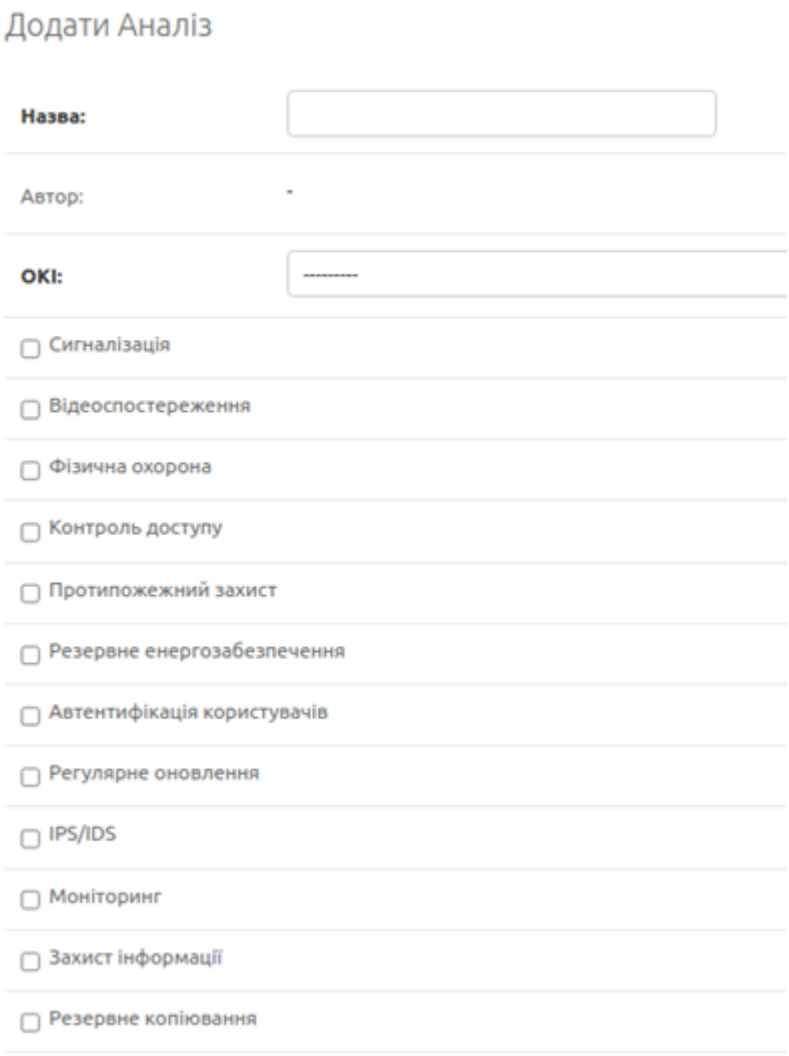



Рисунок 3.4 – Введення інформації про стан захищеності об’єкта

Розроблений інтерфейс орієнтований на моделі даних, де користувачі, в залежності від ролі, отримують доступ до таблиць, передбачених їхніми дозволами. Інтерфейс надає можливість виконувати над записами таблиці сортування, фільтрацію, текстовий пошук у визначених полях. Також, користувач може відмітити один або декілька записів і виконати запрограмовану дію над обраними записами.

В залежності від ролі, користувач отримує кабінет, у якому область видимості таблиць і дозволених дій обмежена згідно його доступу.

Наприклад, аналітик може бачити тільки таблиці з розділу «Інформаційний ресурс», при цьому, він може створювати записи в таблиці Аналізи, а дані інших таблиць – тільки переглядати.

Створені аналітичні звіти за різними критеріями.

Графіки кількісті об’єктів: за населеними пунктами, за районами і провайдерами (рис. 3.5 – 3.7).

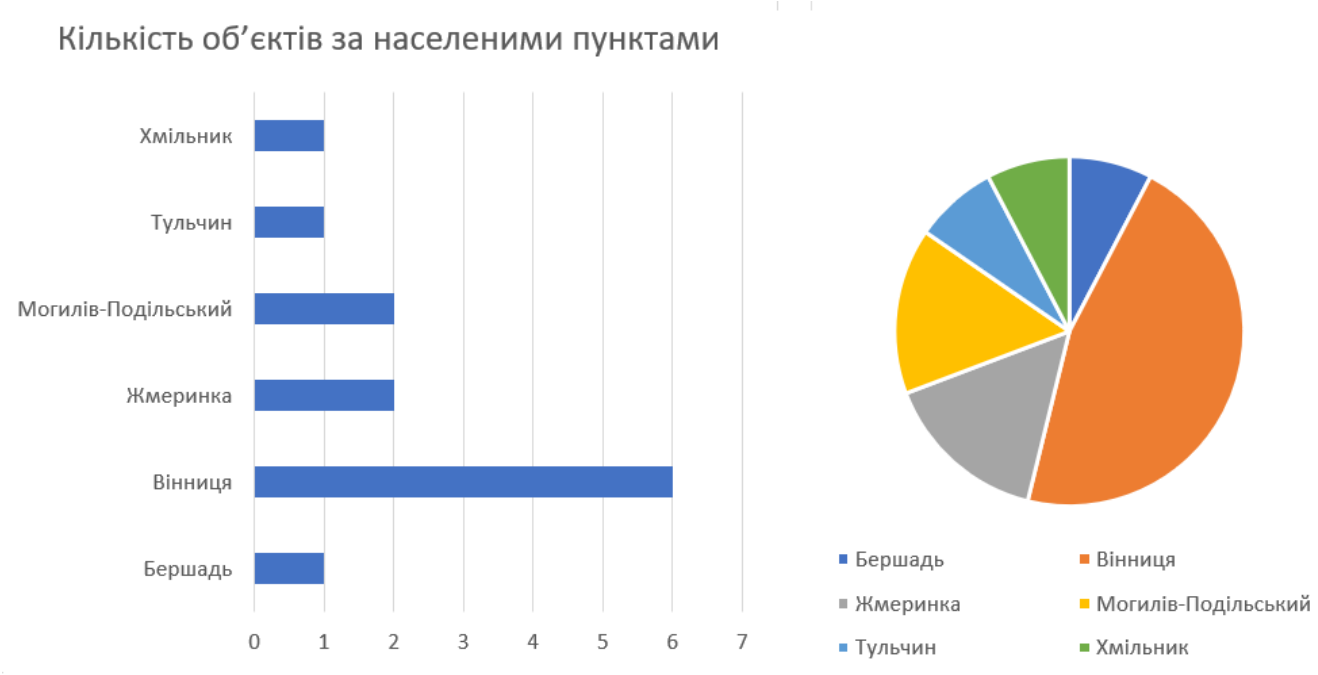



Рисунок 3.5 – Кількість об’єктів за населеними пунктами

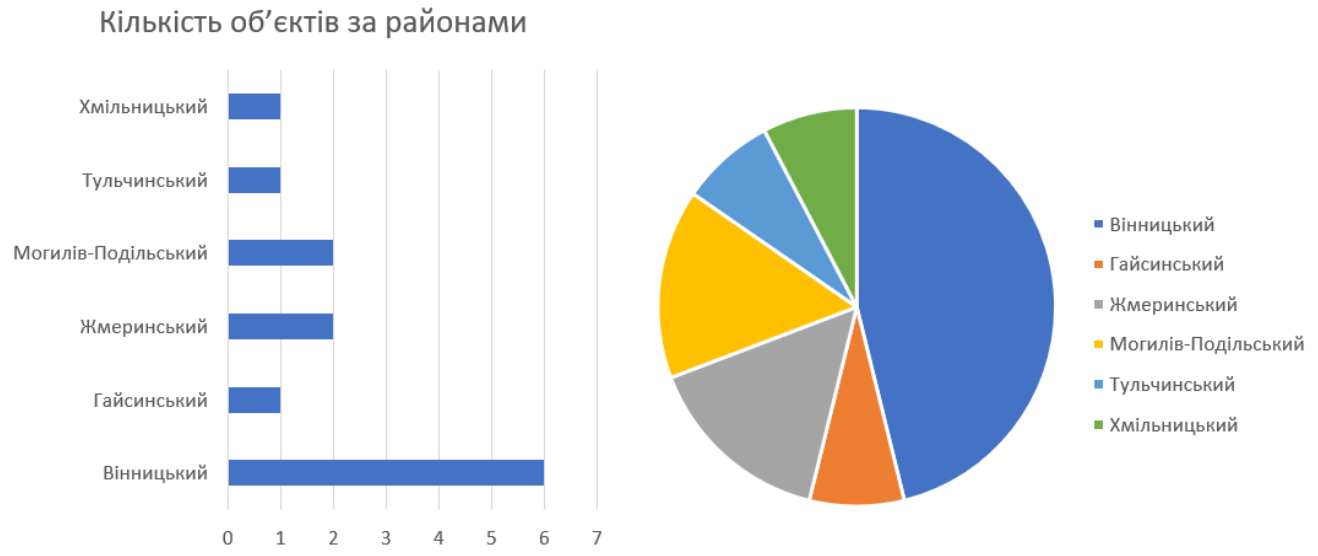



Рисунок 3.6 – Кількість об’єктів за районами

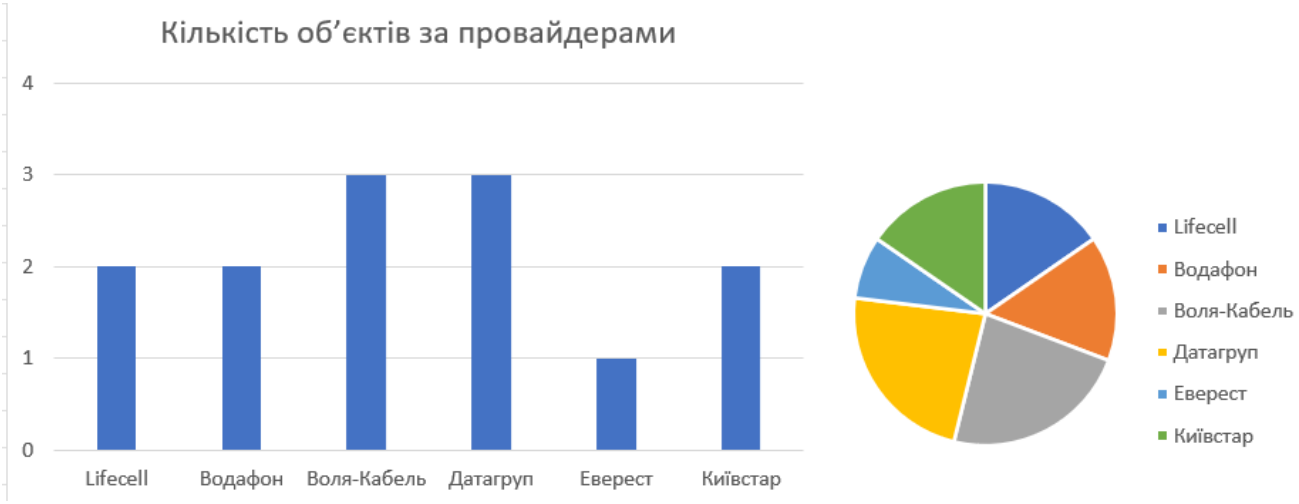



Рисунок 3.7 – Кількість об’єктів за провайдерами

Стан рівня впровадження кіберзахисту і розподіл об’єктів за категоріями критичності (рис. 3.8 – 3.9).

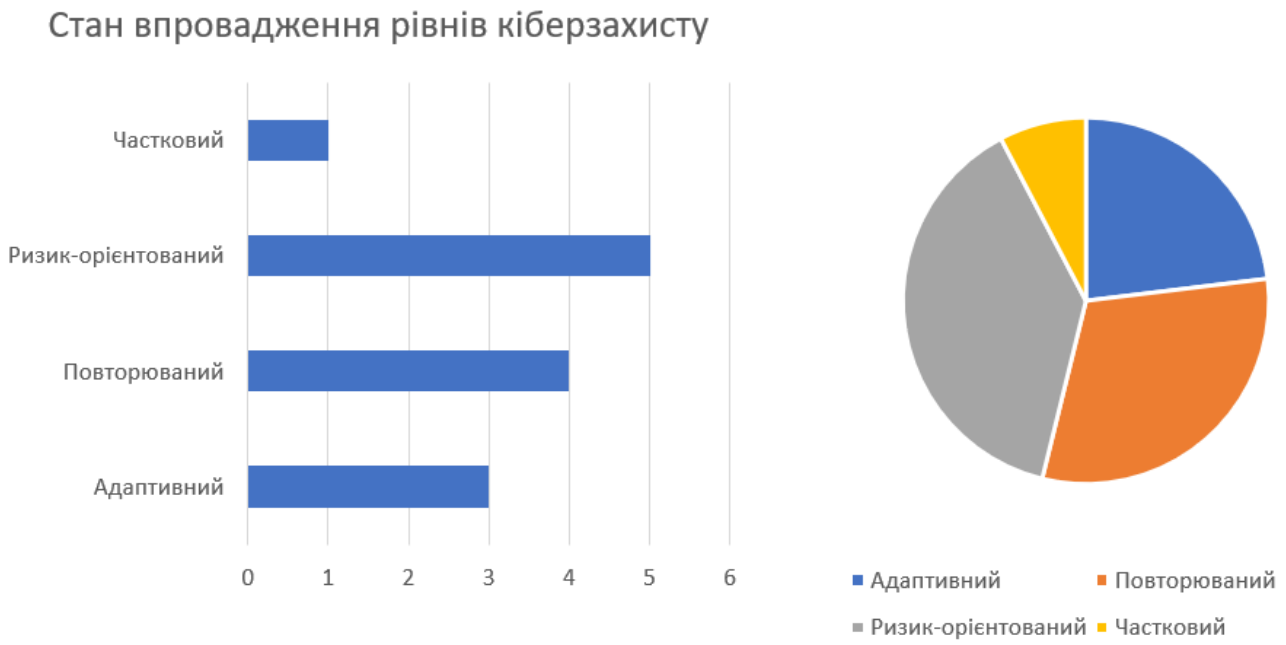



Рисунок 3.8 – Стан впровадження рівнів кіберзахисту


Рисунок 3.9 – Розподіл об’єктів за категоріями критичності

Графік оцінки захищеності провайдерів розраховується як середня оцінка за всіма їх об’єктами (рисунок 3.10):


Рисунок 3.10 – Оцінка захищеності провайдерів

Графік аналітичного звіту стану захищеності об'єктів інформаційно-телекомунікаційної інфраструктури регіону (рисунок 3.11):

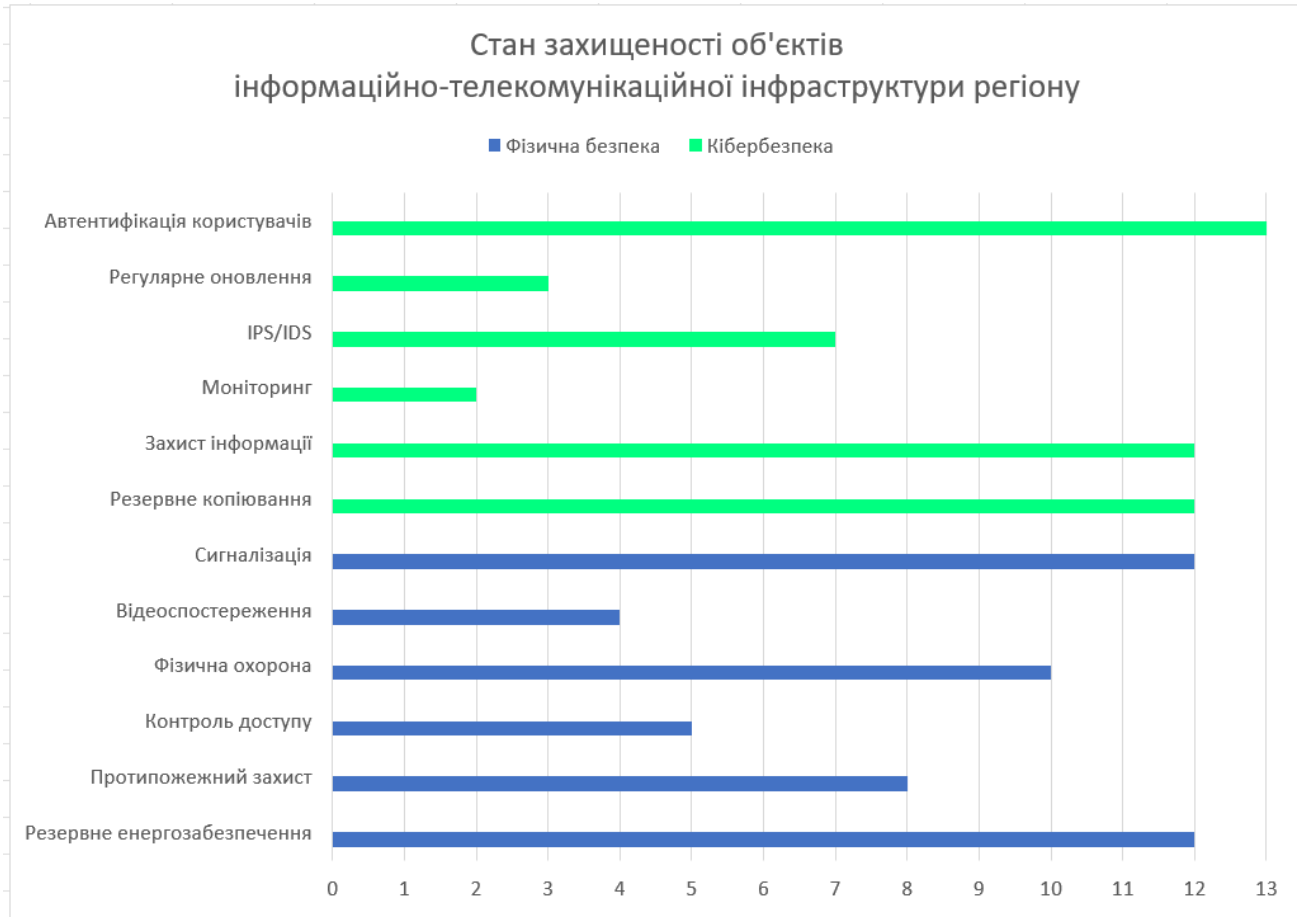



Рисунок 3.11 – Стан захищеності об'єктів інформаційно-телекомунікаційної інфраструктури регіону

### 3.5 Висновки до розділу

У цьому розділі було досліджено і успішно розроблено консолідований інформаційний ресурс аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону.

Для реалізації ресурсу було обрано базу даних PostgreSQL, мову програмування Python та веб-фреймворк Django через їх надійність, зручність і широке застосування у сфері веб-розробки.

Реалізовано базу даних, розроблені механізми захисту ресурсу.

На основі створеного інформаційного ресурсу проведено системний аналіз і отримані висновки безпеки критичних об’єктів інформаційно-телекомунікаційної інфраструктури регіону у вигляді аналітичних звітів.

# РОЗДІЛ IV. ЕКОНОМІЧНА ЧАСТИНА

Важливою складовою процесу науково-дослідної розробки, створення нового продукту або технології є її економічна частина. Вона є значущим елементом, який допомагає визначити комерційний успіх та доцільність впровадження.

Головною метою економічної частини науково-дослідної розробки «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» є оцінка комерційного потенціалу проекту, яка включає в себе аналіз ринкових умов та конкурентного середовища, визначення потенційної користі та ризиків впровадження розробки, розрахунок економічної ефективності та інші фактори, які впливають на успішність проекту.

Магістерська кваліфікаційна робота за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок, тобто коли відбувається комерціалізація науково-технічної розробки. Це пріоритетний напрямок тому, що результатами розробки можуть скористатись інші споживачі, отримуючи при цьому певну економічну вигоду.

Для такого випадку необхідно виконати наступні етапи робіт:

а) проведення комерційного аудиту науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

б) розрахунок витрат на здійснення науково-технічної розробки;

в) розрахунок економічної ефективності науково-технічної розробки у випадку її впровадження і обґрунтування економічної доцільності комерціалізації потенційним інвестором.

## 4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» є отримання оцінки науково-технічного рівня та рівня комерційного потенціалу розробки.

Рекомендовано здійснювати оцінювання науково-технічного рівня розробки та її комерційного потенціалу із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1 [52].

Таблиця 4.1 - Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

| Бали (за 5-ти бальною шкалою) | | | | | |
|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 |
| Технічна здійсненність концепції | | | | | |
| 1 | Достовірність концепції не підтверджена | Концепція підтверджена експертними висновками | Концепція підтверджена розрахунками | Концепція перевірена на практиці | Перевірено працездатність продукту в реальних умовах |
| Ринкові переваги (недоліки) | | | | | |
| 2 | Багато аналогів на малому ринку | Мало аналогів на малому ринку | Кілька аналогів на великому ринку | Один аналог на великому ринку | Продукт не має аналогів на великому ринку |
| 3 | Ціна продукту значно вища за ціни аналогів | Ціна продукту дещо вища за ціни аналогів | Ціна продукту приблизно дорівнює цінам аналогів | Ціна продукту дещо нижче за ціни аналогів | Ціна продукту значно нижче за ціни аналогів |
| 4 | Технічні та споживчі властивості продукту значно гірші, ніж в | Технічні та споживчі влас-тивості продукту трохи гірші, ніж в аналогів | Технічні та споживчі властивості продукту на рівні аналогів | Технічні та споживчі властивості продукту трохи кращі, ніж в | Технічні та споживчі властивості продукту значно кращі, ніж в |
| 5 | Експлуатаційні витрати значно вищі, ніж в аналогів | Експлуатаційні витрати дещо вищі, ніж в аналогів | Експлуатаційні витрати на рівні експлуатаційних витрат аналогів | Експлуатаційні витрати трохи нижчі, ніж в аналогів | Експлуатаційні витрати значно нижчі, ніж в аналогів |

Продовження табл. 4.1

| | | | | | |
|---|---|---|---|---|---|
| Ринкові перспективи | | | | | |
| 6 | Ринок малий і не має позитивної динаміки | Ринок малий, але має позитивну динаміку | Середній ринок з позитивною динамікою | Великий стабільний ринок | Великий ринок з позитивною динамікою |
| 7 | Активна конкуренція великих компаній на ринку | Активна конкуренція | Помірна конкуренція | Незначна конкуренція | Конкурентів немає |
| Практична здійсненність | | | | | |
| 8 | Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї | Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців | Необхідне незначне навчання фахівців та збільшення їх штату | Необхідне незначне навчання фахівців | Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї |
| 9 | Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні | Потрібні незначні фінансові ресурси. Джерела фінансування відсутні | Потрібні значні фінансові ресурси. Джерела фінансування є | Потрібні незначні фінансові ресурси. Джерела фінансування є | Не потребує додаткового фінансування |
| 10 | Необхідна розробка нових матеріалів | Потрібні матеріали, що використовуються у військово промисловому комплексі | Потрібні дорогі матеріали | Потрібні досяжні та дешеві матеріали | Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві |
| 11 | Термін реалізації ідеї більший за 10 років | Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років | Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років | Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років | Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років |
| 12 | Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту | Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу | Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу | Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту | Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту |

Дані результатів оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно додати до таблиці 4.2.

Таблиця 4.2 - Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

| Критерії | Експерт (ПІБ, посада) | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| | Бали: | | |
| 1. Технічна здійсненність концепції | 4 | 4 | 4 |
| 2. Ринкові переваги (наявність аналогів) | 4 | 4 | 4 |
| 3. Ринкові переваги (ціна продукту) | 4 | 3 | 4 |
| 4. Ринкові переваги (технічні властивості) | 4 | 4 | 4 |
| 5. Ринкові переваги (експлуатаційні витрати) | 3 | 3 | 3 |
| 6. Ринкові перспективи (розмір ринку) | 4 | 4 | 3 |
| 7. Ринкові перспективи (конкуренція) | 4 | 4 | 4 |
| 8. Практична здійсненність (наявність фахівців) | 3 | 3 | 4 |
| 9. Практична здійсненність (наявність фінансів) | 3 | 4 | 4 |
| 10. Практична здійсненність (необхідність нових матеріалів) | 4 | 4 | 4 |
| 11. Практична здійсненність (термін реалізації) | 4 | 4 | 4 |
| 12. Практична здійсненність (розробка документів) | 3 | 3 | 3 |
| Сума балів | 44 | 44 | 45 |
| Середньоарифметична сума балів $СБ_c$ | 44,3 | | |

Можемо зробимо висновки щодо науково-технічного рівня і рівня комерційного потенціалу розробки за результатами розрахунків, наведених в таблиці 4.2, для чого скористаємось рекомендаціями, наведеними в табл. 4.3 [52].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

| Середньоарифметична сума балів СБ, розрахована на основі висновків | Науково-технічний рівень та комерційний потенціал розробки |
|---|---|
| 41…48 | Високий |
| 31…40 | Вище середнього |
| 21…30 | Середній |
| 11…20 | Нижче середнього |
| 0…10 | Низький |

Рівень комерційного потенціалу розробки за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону», згідно проведених досліджень, становить 44,3 бала, і відповідно до таблиці 4.3, свідчить, що є комерційна важливість проведення даних досліджень, тобто наявний високий рівень комерційного потенціалу розробки.

### 4.2 Оцінювання рівня новизни розробки

Оцінювання рівня новизни розробки є процесом визначення ступеня оригінальності та унікальності конкретного продукту, технології чи ідеї і є важливим етапом у процесі розробки будь-якого продукту чи послуги.

Визначення рівня і ступеня інтегральної новизни є найбільш актуальним, оскільки її рівень визначає ступінь однакового позитивного сприйняття новизни розробки як виробником, так і споживачем, а отже і ринком в цілому, а це, у свою чергу, є гарантією того, що новинка знайде своє місце на ринку, користуватиметься попитом у споживачів і забезпечить відшкодування витрат, зазнаних виробником під час розроблення та виробництва [53].

Рівень новизни нового продукту розраховується експертним методом шляхом протиставлення нового продукту та його аналогів, які присутні в даний час на ринку, використовуючи чинники, що визначають її значення, за системою

«краще-гірше». Рівень новизни встановлюється відносно рівня аналога, або досить близького до аналога продукту.

Для визначення *i*-го виду новизни застосовуються чинники, які впливають на її рівень. Кожен чинник *i*-го виду новизни розраховується в балах - чим більша кількість набраних балів, тим більший рівень новизни. Для оцінювання рівня новизни використаємо експертів, які встановлюють бали відповідним чинникам. Бал відповідності вноситься в діапазоні від -5 (значно гірше аналога) до +5 (значно краще аналога). Результати оцінювання науково-технічного рівня та комерційного потенціалу розробки зведемо до відповідного листа оцінювання рівня новизни експертами (таблиця 4.4).

Таблиця 4.4 – Лист оцінювання рівня новизни експертами

| Види та чинники | | Бали та експерти | | |
|---|---|---|---|---|
| | | Експерт 1 | Експерт 2 | Експерт 3 |
| 1 | | 2 | 3 | 4 |
| Споживча новизна | Питома вага 0,225 | Максимальний бал $Б_{i\ MAX}$ | | 25 |
| 1. Зміна поведінкових звичок споживача | | 5 | 5 | 4 |
| 2. Ступінь задоволення потреб і запитів | | 5 | 4 | 4 |
| 3. Спосіб задоволення потреби | | 3 | 4 | 4 |
| 4. Формування нової потреби | | 1 | 2 | 1 |
| 5. Формування нового споживача | | 0 | 0 | 0 |
| Середній бал експертів $Б_{i\ отр}$ | | 14 | | |
| Товарна новизна | Питома вага 0,217 | Максимальний бал $Б_{i\ MAX}$ | | 30 |
| 1. Параметричні зміни показників продукції | | | | |
| 1.1. Якісні | | 3 | 4 | 4 |
| 1.2. Технічні | | 4 | 4 | 3 |
| 1.3. Економічні | | 3 | 3 | 4 |
| 1.4. Сервісні | | 4 | 4 | 4 |
| 2. Якість продукції по відношенню до конкурентів | | 3 | 3 | 3 |
| 3. Функціональні зміни | | 3 | 3 | 3 |
| Середній бал експертів $Б_{i\ отр}$ | | 21 | | |

Продовження табл. 4.4

| | | | | |
|---|---|---|---|---|
| Виробнича новизна | Питома вага 0,042 | Максимальний бал $Б_{i\ MAX}$ | | 25 |
| 1. Рівень унікальності товару для підприємства | | 5 | 5 | 5 |
| 2. Рівень унікальності для галузі | | 3 | 4 | 3 |
| 3. Рівень унікальності товару для країни | | 2 | 2 | 1 |
| 4. Зміна виробничої системи | | 4 | 4 | 4 |
| 5. Відносно існуючого асортименту | | 2 | 2 | 2 |
| Середній бал експертів $Б_{i\ отр}$ | | 16 | | |
| Прогресивна новизна | Питома вага 0,179 | Максимальний бал $Б_{i\ MAX}$ | | 25 |
| 1. Зміна технології виготовлення | | 4 | 4 | 4 |
| 2. Рівень застосування нових компонентів і матеріалів | | 1 | 2 | 2 |
| 3. Зміна технологічного принципу дії виробу | | 1 | 2 | 1 |
| 4. Зміна конструктивного виконання | | 2 | 2 | 2 |
| 5. Рівень застосування інновацій | | 2 | 2 | 2 |
| Середній бал експертів $Б_{i\ отр}$ | | 11 | | |
| Ринкова новизна | Питома вага 0,12 | Максимальний бал $Б_{i\ MAX}$ | | 20 |
| 1. Новий виріб на новому ринку | | 0 | 0 | 0 |
| 2. Новий виріб на відомому ринку | | 2 | 2 | 2 |
| 3. Модернізований виріб | | 2 | 2 | 2 |
| 4. Нова модель | | 2 | 2 | 2 |
| Середній бал експертів $Б_{i\ отр}$ | | 6 | | |
| Екологічна новизна | Питома вага 0,035 | Максимальний бал $Б_{i\ MAX}$ | | 20 |
| 1. Рівень екологічної чистоти технології виробництва | | 5 | 5 | 5 |
| 2. Рівень впровадження мало- та безвідходних технологій | | 5 | 5 | 5 |
| 3. Рівень екологічно небезпечних режимів експлуатації продукції | | 5 | 5 | 5 |
| 4. Рівень забруднення навколишнього середовища | | 5 | 5 | 5 |
| Середній бал експертів $Б_{i\ отр}$ | | 20 | | |

Продовження табл. 4.4

| Соціальна новизна | Питома вага 0,036 | Максимальний бал $Б_{i\ MAX}$ | | 20 |
|---|---|---|---|---|
| 1. Використання нового товару приводить до покращення стану здоров'я нації | | 0 | 0 | 0 |
| 2. Використання нового товару приводить до зростання доходів населення | | 0 | 0 | 0 |
| 3. Виробництво нового товару приводить до збільшення (зменшення) кількості робочих місць на підприємстві | | 4 | 4 | 4 |
| 4. Виробництво нового товару приводить до підвищення кваліфікації персоналу | | 3 | 3 | 3 |
| Середній бал експертів $Б_{i\ отр}$ | | 7 | | |
| Маркетингова новизна | Питома вага 0,146 | Максимальний бал $Б_{i\ MAX}$ | | 20 |
| 1. Нові методи маркетингових досліджень | | 0 | 0 | 0 |
| 2. Вживання нових стратегій сегментації ринку | | 3 | 3 | 2 |
| 3. Вибір нової маркетингової стратегії обхвату і розвитку цільового сегмента | | 2 | 3 | 2 |
| 4. Побудова нових каналів збуту | | 2 | 2 | 2 |
| Середній бал експертів $Б_{i\ отр}$ | | 7 | | |

Значення *i*-го виду новизни розраховується за формулою [53]:

$$I_i = \frac{Б_{i\,отр}}{Б_{i\,MAX}}, \tag{4.1}$$

де $Б_{i\ отр}$ – отримана кількість балів за шкалою оцінок чинників, що визначають *i*-й вид новизни;

$Б_{i\ MAX}$ – максимальна кількість балів, що може бути отримана за *i*-м видом новизни.

Загальний рівень інтегральної новизни розраховується як додаток отриманого значення *i*-го виду новизни і її вагомості. Вагомість *i*-го виду новизни визначаємо експертним методом, за формулою [53]:

$$N_{інт} = \sum_{i}^{n} W_i \cdot I_i\ , \tag{4.2}$$

де $N_{інт}$ – рівень інтегральної (сукупної) новизни;

$W_i$ – вагомість (питома вага) $i$-го виду новизни;

$n$ – загальна кількість видів новизни.

$$N_{інт} = (0{,}225 \cdot 14/25)+(0{,}217 \cdot 21/30)+(0{,}042 \cdot 16/25)+(0{,}179 \cdot 11/25)+(0{,}12 \cdot 6/20)+ (0{,}035 \cdot 20/20)+(0{,}036 \cdot 7/20)+(0{,}146 \cdot 7/20) = 0{,}518.$$

Отримане значення інтегрального рівня новизни зіставляємо зі шкалою, що наведена в табл. 4.5 [52].

Таблиця 4.5 – Рівні новизни нового товару та їхня характеристика

| Рівні новизни товару | Значення інтегральної новизни | Характеристика товару | Вид нового товару |
|---|---|---|---|
| Найвища | 1,00 | Абсолютно новий товар | Новий товар, що наділений ознаками інноваційності (інноваційний товар) |
| Висока | 0,8…0,99 | Товар, який не має аналогів | |
| Значуща | 0,6…0,79 | Принципова зміна споживчих властивостей товару | |
| Достатня | 0,4…0,59 | Принципова технологічна модифікація товару | |
| Незначна | 0,2…0,39 | Кардинальна зміна параметрів | Новий товар |
| Помилкова | 0,00…0,19 | Малоістотна модифікація | |

Відповідно до таблиці 4.5, отримане значення інтегральної новизни: 0,518. Це показує, що розробка відповідає таким рівням:

- рівень новизни товару – достатня новизна;
- характеристика – принципова технологічна модифікація товару;

- вид розробки – новий товар, що наділений ознаками інноваційності (інноваційний товар).

### 4.3 Розрахунок витрат на проведення науково-дослідної роботи

Необхідно згрупувати за відповідними статтями витрати, які пов’язані з проведенням науково-дослідної роботи на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» під час планування, обліку і калькулювання собівартості.

#### 4.3.1 Витрати на оплату праці

Статті «Витрати на оплату праці» включає в себе витрати на виплату основної та додаткової заробітної плати працівникам, які безпосередньо задіяні у виконанні розробки, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці. Такими працівникам можуть бути керівники відділів, наукові, інженерно-технічні працівники, конструктори, технологи і інші працівники.

Основна заробітна плата дослідників. Витрати на основну заробітну плату дослідників ($З_о$) розраховуються у відповідності до посадових окладів працівників, за формулою [52]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.3)$$

де $k$ – кількість посад дослідників залучених до процесу досліджень;

$M_{ni}$ – місячний посадовий оклад конкретного дослідника, грн;

$t_i$ – число днів роботи конкретного дослідника, дні;

$T_p$ – середнє число робочих днів в місяці, $T_p$=24 дні.

$$З_о = 19000{,}00 \cdot 60 / 24 = 47500{,}00 \text{ грн.}$$

Проведені розрахунки вносяться до таблиці 4.6.

Таблиця 4.6 – Витрати на заробітну плату дослідників

| Найменування посади | Місячний посадовий оклад, грн | Оплата за робочий день, грн | Число днів роботи | Витрати на заробітну плату, грн |
|---|---|---|---|---|
| Керівник проекту | 19000,00 | 791,67 | 60 | 47500,00 |
| Інженер-розробник програмного забезпечення | 17000,00 | 708,33 | 56 | 39666,67 |
| Науковий співробітник дослідження проблем програмного забезпечення | 13000,00 | 541,67 | 10 | 5416,67 |
| Всього | | | | 92583,33 |

Основна заробітна плата робітників.

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» розраховується за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i \,, \tag{4.4}$$

де $C_i$ – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

$t_i$ – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду $C_i$ можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \,, \tag{4.5}$$

де $M_M$ – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

$K_i$ – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду [52];

$К_с$ – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

$Т_р$ – середнє число робочих днів в місяці, приблизно $Т_р$ = 24 дні;

$t_{зм}$ – тривалість зміни, год.

$$С_1 = 6700,00 \cdot 1,10 \cdot 1,65 / (24 \cdot 8) = 63,34 \text{ грн.}$$

$$З_{р1} = 63,34 \cdot 6,00 = 380,02 \text{ грн.}$$

Таблиця 4.7 – Величина витрат на основну заробітну плату робітників

| Найменування робіт | Тривалість роботи, год | Розряд роботи | Тарифний коефіцієнт | Погодинна тарифна ставка, грн | Величина оплати на робітника грн |
|---|---|---|---|---|---|
| Установка електронно-обчислювального обладнання | 6 | 2 | 1,1 | 63,34 | 380,02 |
| Підготовка робочого місця дослідника | 2,4 | 2 | 1,1 | 63,34 | 152,01 |
| Інсталяція програмного забезпечення | 2,2 | 5 | 1,7 | 97,88 | 215,34 |
| Всього | | | | | 747,36 |

Додаткова заробітна плата дослідників та робітників

Додаткова заробітна плата розраховується як 10-12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.6)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймаємо 10%.

$З_{дод}$ = (92583,33+ 747,36) · 10 / 100% = 9333,07 грн.

### 4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.7)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

*Зн* = (92583,33+ 747,36+ 9333,07) · 22 / 100% = 22586,03 грн.

### 4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{вj}\ , \quad (4.8)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

*n* – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 ... 1,15*);

$В_j$ – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1$ = 2,00 · 200,00 · 1,1 - 0,000 · 0,00 = 440,0 грн.

Проведені розрахунки зведемо до таблиці 4.8.

Таблиця 4.8 – Витрати на матеріали

| Найменування матеріалу, марка, тип, сорт | Ціна за од, грн | Норма витрат, од | Величина відходів, кг | Ціна відходів, грн/кг | Вартість витраченого матеріалу, грн |
|---|---|---|---|---|---|
| Офісний папір, уп | 200,00 | 2 | 0 | 0 | 440,00 |
| Папір для записів, уп | 110,00 | 1 | 0 | 0 | 121,00 |
| Органайзер офісний,шт | 210,00 | 2 | 0 | 0 | 462,00 |
| Канцелярське приладдя (набір офісного працівника), шт | 175,00 | 2 | 0 | 0 | 385,00 |
| Картридж для принтера | 1100,00 | 1 | 0 | 0 | 1210,00 |
| Диск оптичний CD-RW | 15,00 | 3 | 0 | 0 | 49,50 |
| Flesh-пам'ять 16 GB | 130,00 | 1 | 0 | 0 | 143,00 |
| Тека для паперів | 82,00 | 2 | 0 | 0 | 180,40 |
| Всього | | | | | 3490,63 |

### 4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» відсутні.

### 4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування, яке необхідне для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування та встановлення. В дослідній роботі «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» витрати на спец устаткування відсутні.

### 4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та, за потреби, придбання спеціальних програмних засобів і програмного забезпечення, які необхідні для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансова вартість програмного забезпечення розраховується за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.9)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

$K_i$ – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

$k$ – кількість найменувань програмних засобів.

$B_{прг} = 5399,00 \cdot 1 \cdot 1,12 = 6046,88$ *грн.*

Отримані результати вносяться до таблиці 4.9.

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

| Найменування програмного засобу | Кількість, шт | Ціна за одиницю, грн | Вартість, грн |
|---|---|---|---|
| ОС Windows 11 | 1 | 5399 | 6046,88 |
| Прикладний пакет Microsoft Office 2019 | 1 | 5290 | 5924,80 |
| Система розробки PyCharm 2023 | 1 | 11100 | 12432,00 |
| Всього | | | 24403,68 |

### 4.3.7 Амортизація обладнання, програмних засобів та приміщень

Для спрощення, амортизаційні відрахування по кожному виду обладнання та програмному забезпеченню, розраховуються з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.10)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

*$A_{обл}$ = (24500,00 · 2) / (2 · 12) = 2041,67 грн.*

Проведені розрахунки вносяться до таблиці 4.10.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

| Найменування обладнання | Балансова вартість, грн | Строк корисного використання, років | Термін використання обладнання, місяців | Амортизаційні відрахування, грн |
|---|---|---|---|---|
| Персональний комп'ютер | 24500,00 | 2 | 2 | 2041,67 |
| Робоче місце дослідника | 7800,00 | 5 | 2 | 260,00 |
| Оргтехніка | 8700,00 | 4 | 2 | 362,50 |
| ОС Windows 11 | 5200,00 | 2 | 2 | 433,33 |
| Прикладний пакет Microsoft Office 2019 | 5000,00 | 2 | 2 | 416,67 |
| Всього | | | | 3514,17 |

### 4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на електричну енергію ($B_e$) розраховуються за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.11)$$

де $W_{yi}$ – встановлена потужність обладнання на визначеному етапі розробки, кВт;

$t_i$ – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e$ = 7,50 грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

$\eta_i$ – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,3 \cdot 452,0 \cdot 7,50 \cdot 0,95 / 0,97 = 996,03$ *грн.*

Проведені розрахунки вносяться до таблиці 4.11.

Таблиця 4.11 – Витрати на електроенергію

| Найменування обладнання | Встановлена потужність, кВт | Тривалість роботи, год | Сума, грн |
|---|---|---|---|
| Персональний комп'ютер | 0,3 | 452 | 996,03 |
| Робоче місце дослідника | 0,15 | 452 | 498,02 |
| Оргтехніка | 0,45 | 10 | 33,05 |
| Всього | | | 1527,10 |

### 4.3.9 Службові відрядження

Службові відрядження - це поїздки співробітників організації за межі місця їх постійної роботи для виконання службових обов'язків.

До статті «Службові відрядження» дослідної роботи на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-

телекомунікаційної інфраструктури регіону» належать витрати на відрядження штатних працівників, працівників організацій, аспірантів, зайнятих розробленням досліджень, витрати на відрядження на наукові конференції, наради, які пов'язані з виконанням досліджень.

Витрати за статтею «Службові відрядження» розраховується як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.12)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

*$B_{св}$ = (92583,33+ 747,36) · 20 / 100% = 18666,14 грн.*

### 4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуються як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.13)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

*$B_{сп}$ = (92583,33+ 747,36) · 30 / 100% = 27999,21 грн.*

### 4.3.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

*$I_в$ = (92583,33+ 747,36) · 50 / 100% = 46665,35 грн.*

### 4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 120%.

*$В_{нзв}$ = (92583,33+ 747,36) · 120 / 100% = 111996,83 грн.*

Витрати на проведення науково-дослідної роботи на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.17)$$

*$В_{заг}$=92583,33+747,36+9333,07+22586,03+3490,63+0,00+0,0+24403,68+3514,17 +1527,10+18666,14+27999,21+46082,01+111996,83= 363512,89 грн.*

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.16)$$

де $\eta$ - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо $\eta$=0,9.

$$ЗВ = 363512,89/\ 0,9 = 403903,21\ грн.$$

## 4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

Узагальнюючий позитивний результат, що може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$\Delta N$ – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

| Показник | 1-й рік | 2-й рік | 3-й рік | 4-й рік |
|---|---|---|---|---|
| Збільшення кількості споживачів, проектних груп | 500 | 700 | 700 | 400 |

$N$ – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 100 проектних груп;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 15000,00 грн;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 1000,00 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [52]:

$$\Delta П_i = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.17)$$

де $\lambda$ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

$\rho$ – коефіцієнт, який враховує рентабельність інноваційного продукту. Приймемо $\rho$ =38%;

$\vartheta$ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1$ =(1000,00·100+16000,00·500)·0,83·0,38·(1-0,18/100%)= 2550141,47 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2$ =(1000,00·100+16000,00·(500+700))·0,83·0,38·(1-0,18/100%)= 6076263,00грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3$ =(1000,00·100,00+16000,00·(500+700+700))·0,83·0,38·(1-0,18/100%)= 9602384,54 грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4$ =(1000,00·100,00+21000,00·(500+700+700+400))·0,83·0,38·(1-0,18/100%)= 11617311,13 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.18)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

$T$ – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

$\tau$ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau$ =0,25;

$t$ – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

*ПП* =2550141,47 /(1+0,25)$^1$+ 6076263,00 /(1+0,25)$^2$+ 9602384,54 /(1+0,25)$^3$+ +11617311,13 /(1+0,25)$^4$= 59799071,08 грн.

Величина початкових інвестицій $PV$, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \quad (4.19)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$ =2;

*ЗВ* – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 403903,21 грн.

$PV = k_{інв} \cdot ЗВ = 2 \cdot 403903{,}21 = 807806{,}42$ грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \tag{4.20}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 59799071,08 грн;

$PV$ – теперішня вартість початкових інвестицій, 807806,42 грн.

$E_{абс} = ПП - PV = 59799071{,}08 - 807806{,}42 = 58991264{,}66$ грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.21}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 12612807,79 грн;

$PV$ – теперішня вартість початкових інвестицій, 798589,26 грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+58991264{,}66 / 807806{,}42)^{1/4} - 1 = 1{,}93.$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f\,, \tag{4.22}$$

де $d$ – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні $d$ =0,11;

$f$ – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,2.

$\tau_{мін}$= 0,11+0,2 = 0,31 < 1,93 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}\,, \tag{4.23}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 1,93 = 0,52 року.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

### 4.5 Висновки до розділу

Згідно проведених досліджень розробки за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-

телекомунікаційної інфраструктури регіону» рівень комерційного потенціалу становить 44,3 бала, що свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

Також термін окупності становить 0,52 року, що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

На підставі отриманих розрахунків можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону».

# ВИСНОВКИ

У даній магістерській кваліфікаційній роботі було проведено дослідження та розробку на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону».

Розроблений "Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону" є досить значимим інструментом для виявлення, аналізу та управління ризиками в інформаційно-телекомунікаційних системах регіону. Даний ресурс має декілька основних висновків:

1. Інструмент забезпечує цілісний погляд на загальну безпеку інформаційно-телекомунікаційної інфраструктури регіону, охоплюючи всі аспекти її захисту.

2. Ресурс дозволяє проводити системний аналіз безпеки, ідентифікувати можливі загрози, визначати уразливості та оцінювати ризики, пов'язані з інформаційно-телекомунікаційною інфраструктурою регіону.

3. За допомогою ресурсу можна розробляти та впроваджувати заходи щодо запобігання та обмеження ризиків, а також відновлення систем після інцидентів безпеки.

4. Ресурс має гнучку структуру, що дозволяє адаптувати його до конкретних потреб та характеристик інформаційно-телекомунікаційної інфраструктури регіону.

5. Впровадження розробленого ресурсу може сприяти поліпшенню загальної безпеки інформаційно-телекомунікаційної інфраструктури регіону, зменшенню впливу можливих загроз та покращенню реагування на інциденти.

Загалом, розроблений "Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону" має великий потенціал для забезпечення безпеки інформаційно-телекомунікаційної інфраструктури регіону та зростання стійкості до можливих загроз.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова КМУ від 23.08.2016 р. № 563 . Офіційний вісник України. 2016. №69.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс] // Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

3. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX [Електронний ресурс] // Відомості Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20

4. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (зі змінами): Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України, №601 від 06.10.2021. [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601

5. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

6. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України; Порядок, Форма типового документа від 09.10.2020 № 943. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/943-2020-%D0%BF

7. С. Гончар, "Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури", Моделювання та інформаційні технології, Вип. 80, С. 27-32, 2017.

8. Ю. Дрейс, "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави", Захист інформації, Т. 19, № 3, С. 214-222, 2017.

9. A. Leandros, K. Ki-Hyung, J. Helge, "Cruz Cyber security of critical infrastructures", ICT Express, №4, pp. 42-45, 2018.

10. Д. Бірюков, С. Кондратов, О. Суходоля, Зелена книга з питань захисту критичної інфраструктури в Україні, К., 2016, 176 с.

11. В. Козюра, В. Хорошко, "Заходи протидії прихованої передачі інформації в локальних мережах. Актуальні проблеми управління інформаційною безпекою держави", зб. тез наук. доп. наук.-практ. конф., Київ : Нац. акад. СБУ, С. 91-93, 2018.

12. В. Малащенко, "Теоретичні підходи до проблем та сучасних способів захисту від «інсайдерів»", Ефективність державного управління, Вип. 29, 2011.

13. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.

14. М-54 Основи телекомунікації: навчальний посібник / Архипов О.Є., Гулак Г.М., Кащук В.І., Мельник С.В. – К. : Наук.-вид. відділ НА СБ України, 2017. – 237 с.

15. Кісь Я. П. Методи документування консолідованої інформації: навч. посібник /Я. П.Кісь, Р. О.Голощук– Львів: Львівська політехніка, 2010. – 238 с. – ISBN 966-553-995-7

16. Кунанець Н. Е. Вступ до фаху «Консолідована інформація» / Н. Е. Кунанець, В. В. Пасічник. – Львів: Львівська політехніка, 2013. – 196 с. ISBN 978-966-553-975-9

17. Розробка схеми консолідації інформації на великому підприємстві. Н.О. Нещадим Наукові праці НУХТ № 40

18. Калитич Г.І. Консолідація інформації, знань і мудрості як проектування і основа гармонійного поступу України / Г.І. Калити / / НТІ, 2008 № 1

19. А. О.Азарова, А. А.Шиян,С. П.Мурза, А. В.Кудлик, Т. С.Костюк, «Розроблення захищеного консолідованого інформаційного ресурсу аналізу ринку надання послуг медичними лабораторіями в Україні», ВісникХНУ. Технічнінауки, No 6 (279),с. 105-109, 2019.

20. A.Azarova, A. Shiyan, Y.Mironova, L. Shturma, «The development of secured consolidated infor-mation resource of activity analysis of the poultry industry in Ukraine»,Technology audit and produc-tion reserves,No 6/2 (50), pp. 14–18, 2019.

21. Кунанець Н. Е., Пасічник В. В. Вступ до спеціальності «Консолідована інформація». Навчальний посібник — Львів: «Львівська політехніка», 2010. (Серія «Консолідована інформація». Випуск 1). — 196 с

22. С. Гончар, Г. Леоненко, "Аналіз факторів впливу на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури", Information technology and security, Vol. 4, issue 2 (7), С. 262-268, 2016.

23. В. Мохор, С. Гончар, О. Дибач, "Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури", Ядерна та радіаційна безпека, Вип. 2, С. 4-8, 2019.

24. B. Kosko, "Fuzzy Cognitive Maps", International Journal of Man-Machine Studies, Vol. 24, No. 1, pp. 65-75, 1986.

25. О. М. Степанова, А. А. Волков, «Оцінка інформаційних ризиків в умовах розвитку інформаційної системи підприємства», Вісник східноукраїнського національного університету імені В. Даля, №10 (240), с.106-110, 2017.

26. І. С. Добринін, Н. О. Мальцева, «Вдосконалення методики факторного аналізу інформаційних ризиків», Системи обробки інформації, Вип.3 (149), с.146-150, 2017.

27. О. Г. Корченко, С. В. Казмірчук, «Метод оцінювання ризиків інформаційної безпеки на основі відкритих баз даних уразливостей», Безпека інформації, т.22, №2, с.214-224, 2016.

28. Ю. М. Ткач, С.В. Казмірчук та ін., «Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу», Захист інформації, т.19, №2, с.137-142, 2017.

29. Салієва О.В. Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп’ютерної мережі / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 21, №4, 2019. – С. 28–39.

30. Салієва О.В. Когнітивна модель для дослідження рівня захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №2, 2020. – С. 64–73.

31. Салієва О.В. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №1, 2020. – С. 42–49.

32. Салієва О.В. Визначення допустимої інтенсивності зниження рівня захищеності об’єкта критичної інфраструктури ранжуванням загроз / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 22, №2, 2020. – С. 63–76.

33. Салієва О.В. Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Захист інформації. – Т. 22, №3, 2020. – С. 47–55.

34. Салієва О.В. Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 22, №3, 2020. – С. 59–65.

35. Салієва О.В. Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об’єкту критичної інфраструктури за результатами когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Вісник Черкаського державного технологічного університету. – №3, 2020. – С. 74–83.

36. Салієва О.В. Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи захисту інформації / О.В. Салієва, Ю.Є. Яремчук // Вісник Вінницького політехнічного інституту. – №5, 2020. – С. 47–54.

37. В. М. Богуш, О. А. Довидьков, В. Г. Кривуца, Теоретичні основи захищених інформаційних технологій. К., Україна: ДУІКТ, 2010,454с.

38. Корнієнко С. К. Системи баз даних: організація та проектування: Навчальний посібник / С. К. Корнієнко. – Запоріжжя : ЗНТУ, 2006. – С. 252.

39. А. О. Азарова, А. А. Шиян, і Л. О. Нікіфорова, «Розроблення захищеного консолідованого інформаційного ресурсу аналізу діяльності морських портів України», ІТКІ, вип. 48, вип. 2, с. 27–36, Вер 2020.

40. А. О. Азарова, А. А. Шиян, С. П. Мурза, А. В. Кудлик, Т. С. Костюк, «Розроблення захищеного консолідованого інформаційного ресурсу аналізу ринку надання послуг медичними лабораторіями в Україні», Вісник ХНУ. Технічні науки, No 6 (279),с. 105-109, 2019.

41. A.Azarova, A. Shiyan, Y.Mironova, L. Shturma, «The development of secured consolidated information resource of activity analysis of the poultry industry in Ukraine»,Technology audit and produc-tion reserves,No 6/2 (50), pp. 14–18, 2019.

42. A.Silberschatz, H. F.Korth, S.Sudarshan, Database system concepts. New York, USA: McGraw-Hill, 2011,1349.

43. Гайна Г.А. Основи проектування баз даних: Навчальний посібник / Г.А. Гайна. − К. : КНУБА, 2005. – 204 с.

44. Гайджарж В. І. Основи проектування та використання баз даних: навчальний посібник / В.І. Гайджарж, О.А. Дацюк. – К.: ІВЦ «Видавництво «Політехніка», 2004. – 256 с

45. Гайна Г.А. Організація баз даних і знань. Мови баз даних: Конспект лекцій.−К.:КНУБА, 2002. − 64 с.

46. Гайна Г.А., Попович Н.Л. Організація баз даних і знань. Організація реляційних баз даних: Конспект лекцій.−К.:КНУБА, 2000. − 76 с

47. Бази даних: проектування та реалізація/ Г. С. Погромська, Н.А. Махровська. – Місто: Видавництво, 2019. – 183 с

48. Харів Н. О. Х 20 Бази даних та інформаційні системи: навчльний посібник / Н. О. Харів. – Рівне : НУВГП, 2018. – 127 с.

49. Пасічник В. В., Резніченко В. А. Організація баз даних та знань. – К.: Видавнича група BHV, 2006. – 384 с.: іл

50. Методичні вказівки до виконання курсової роботи з дисципліни «Бази даних і знань» для студентів напряму підготовки 6.170103 «Управління

інформаційною безпекою» / Уклад.: Ю. Є. Яремчук, Д.П. Присяжний, І.О. Дьогтєва. – Вінниця : ВНТУ, 2017. – 25 с.

51. Жежнич П. І. Консолідовані інформаційні ресурси баз даних та знань. - .Львів, Вид. Львівської політехніки, 2010 г. - 212 с.

52. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. Вінниця : ВНТУ, 2021. 42 с.

53. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа. Вінниця : ВНТУ, 2016. 113 с

54. Карпінець В.В. Підвищення стійкості цифрових водяних знаків до геометричних перетворень шляхом визначення особливих точок зображення / В.В. Карпінець, П.В. Павловський, О.В. Салієва, Я.Ю. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 2(36), 2018. – С. 27–36.

55. Шиян А.А. Перспективи використання методів розмежування доступу в інформаційному протиборстві / А. А. Шиян, М. Л. Тюльпін, Я. Ю. Яремчук // Матеріали XII Міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій» (ITSec-2023), м. Ужгород, 2–4 травня 2023 р. – К.: НАУ, 2023. – С. 120–122.

56. Шиян А.А. Метод формування системи захисту від інформаційно-психологічних атак у соціальних мережах / А. А. Шиян, Я. Ю. Яремчук, В. В. Саврацький // Матеріали IX Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем», Львів, 25–26 травня 2023 р. – 2023. – С. 43–44

57. Приймак А.В. Метод автоматизованого пошуку несанкціонованого майнінгу криптовалюти у контейнерах серверних ОС / А.В. Приймак, В.В. Карпінець, Я.Ю. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 2(36), 2020. – С. 16–24.

58. Шиян А.А., Нікіфорова Л.О., Дьогтєва І.О., Яремчук Я.Ю. Модель управління протидією інформаційним атакам в кіберпросторі // Реєстрація, зберігання і обробка даних. – Т. 23, №2, 2021. – С. 62–71.

59. Салієва О.В., Яремчук Я.Ю. Порівняння моделей інформаційної безпеки за характеристиками суб'єктів // Збірник матеріалів 23-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI сторіччі». Том 9. Міжнародна конференція «Управління знаннями та конкурентна розвідка». – Харків, 2019. – С. 67–68.

60. Яремчук Я.Ю. Дослідження можливості підвищення стійкості протоколу автентифікації WPA-PSK // Матеріали XLVIII науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2019) [Електронне мережне наукове видання] : збірник доповідей. – Вінниця : ВНТУ, 2018. – С. 2455–2456.

61. Грицак А.В. Підвищення стійкості віртуальних серверів до DDOS-атак на основі масштабування обчислювальних ресурсів кластера / А. В. Грицак, Я. Ю. Яремчук, В. М. Білоус // Матеріали VI Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології»: тези доповідей, 20-21 квітня 2023 р. – Кропивницький: ЦНТУ, 2023. – С. 83–84.

62. Павловський П.В. Підвищення захисту від несанкціонованого доступу під час голосування в органах державної влади на основі апаратної біометричної ідентифікації голосуючого / П.В. Павловський, Д.П. Присяжний, І.В. Абрамчук, В.В. Саврацький, В.М. Білоус // Вісник Хмельницького національного університету. Серія: Технічні науки. – № 3, 2023. – С. 355–359.

63. Білоус В. М. Системний аналіз безпеки інформаційно-телекомунікаціної інфраструктури регіону на основі захищеного консолідованого інформаційного ресурсу [Електронний ресурс] / В. М. Білоус, Ю. Є. Яремчук // Міжнародна науково-практична інтернет-конференція «Молодь в науці: дослідження, проблеми, перспективи (МН-2024)»: тези доповідей, Вінниця, 2023 р. – Електрон. текст. дані. – 2023. – Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/19804/16773.

# ДОДАТКИ

**Додаток А. Технічне завдання**

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

**ЗАТВЕРДЖУЮ**
Голова секції "Управління інформаційною
безпекою" кафедри МБІС
д.т.н., професор

Юрій ЯРЕМЧУК
"20" Вересня 2023 р.

# ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:
ний консолідований інформаційний ресурс системного аналізу безпеки
інформаційно-телекомунікаційної інфраструктури регіону
08-72.МКР.009.00.000.ТЗ

Керівник магістерської кваліфікаційної роботи

д.т.н., проф.Яремчук Ю.Є.

**1. Найменування та область застосування**

Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону

**2.Підстава для розробки**

Розробка виконується на основі наказу ректора ВНТУ від 18 вересня 2023 року № 247

**3. Мета та призначення розробки**

3.1 Мета розробки: розробка захищеного консолідованого інформаційного ресурсу системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону

3.2 Призначення: консолідація та системний аналіз безпеки інформаційно-телекомунікаційної інфраструктури та захист цих даних.

**4. Джерела розробки**

4.1. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // Сучасний захист інформації. – 2016. №4.– С. 47-51.

4.2. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.4. ZakariaOmar, ZangooeiToomaj, MohdAfiziMohdShukran. Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. IJACT, Vol. 4, No. 15, pp. 189-197, 2012.

**5. Вимоги до програми**

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Pentium 1500 МГц і подібні до них;

– оперативна пам’ять – не менше 512 Mb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп'ютерною технікою.

**6. Вимоги до програмної документації**

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.4

**7. Вимоги до технічного захисту інформації**

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

**8. Техніко-економічні показники**

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

**9. Стадії та етапи розробки**

| № | Назва етапів магістерської кваліфікаційної роботи | Строк виконання етапів роботи | | Примітка |
|---|---|---|---|---|
| 1. | Визначення напрямку магістерської роботи, формулювання теми | 20.09.2023 | 31.09.2023 | |
| 2. | Аналіз предметної області обраної теми | 01.10.2023 | 15.10.2023 | |
| 3. | Розробка роботи | 16.10.2023 | 26.10.2023 | |
| 4. | Написання магістерської роботи на основі розробленої теми | 27.10.2023 | 15.11.2023 | |
| 5. | Передзахист магістерської кваліфікаційної роботи | 16.11.2023 | 24.11.2023 | |
| 6. | Виправлення, уточнення, корегування магістерської кваліфікаційної роботи | 27.11.2023 | 04.12.2023 | |
| 7. | Захист магістерської кваліфікаційної роботи | 11.12.2023 | 17.12.2023 | |

**10. Порядок контролю та прийому**

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– програмний додаток;

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв _____ Білоус В.М.

## Додаток Б. Лістинги програм

system/urls.py
---

```
"""
The `urlpatterns` list routes URLs to views. For more information please see:
    https://docs.djangoproject.com/en/4.2/topics/http/urls/
Examples:
Function views
    1. Add an import:  from my_app import views
    2. Add a URL to urlpatterns:  path('', views.home, name='home')
Class-based views
    1. Add an import:  from other_app.views import Home
    2. Add a URL to urlpatterns:  path('', Home.as_view(), name='home')
Including another URLconf
    1. Import the include() function: from django.urls import include, path
    2. Add a URL to urlpatterns:  path('blog/', include('blog.urls'))
"""

from django.conf import settings
from django.conf.urls.static import static
from django.urls import path, include
from django.views.generic import TemplateView

from core.admin import (
    administrator_admin,
    analyst_admin,
)


urlpatterns = [
    path('', TemplateView.as_view(template_name="admin/home.html")),
    path(settings.ROLE_ADMIN_PATH.get('ADMINISTRATOR'), administrator_admin.urls),
    path(settings.ROLE_ADMIN_PATH.get('ANALYST'), analyst_admin.urls),
    path('users/', include('users.urls')),
]

if settings.DEBUG:
    urlpatterns += static(settings.STATIC_URL, document_root=settings.STATIC_ROOT)
    urlpatterns += static(settings.MEDIA_URL, document_root=settings.MEDIA_ROOT)
    if settings.DEBUG_TOOLBAR:
        urlpatterns += [
            path('__debug__/', include('debug_toolbar.urls')),
        ]


"""
ASGI config for system project.

It exposes the ASGI callable as a module-level variable named ``application``.
```

```
For more information on this file, see
https://docs.djangoproject.com/en/4.2/howto/deployment/asgi/
"""

import os

from django.core.asgi import get_asgi_application

os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'system.settings')

application = get_asgi_application()
```

users/models.py

```
--------------------
from django.db import models
from django.contrib.auth.models import AbstractUser
from django.conf import settings

class User(AbstractUser):
    class Role(models.IntegerChoices):
        ABSENT = 0, 'Немає'
        ADMINISTRATOR = 1, 'Адміністратор'
        ANALYST = 2, 'Аналітик'

    middle_name = models.CharField('По батькові', max_length=50, default='', blank=True)
    phone = models.CharField('Телефон', max_length=30, default='', blank=True)
    role = models.IntegerField('Роль', choices=Role.choices, default=Role.ABSENT, blank=True)

    class Meta:
        verbose_name = 'Користувач'
        verbose_name_plural = 'Користувачі'

    def __str__(self):
        return f'{self.last_name} {self.first_name}'


class LoginLog(models.Model):
    username = models.CharField("Логін", max_length=150, blank=True)
    user = models.ForeignKey(User, models.SET_NULL, verbose_name='Користувач', blank=True,
null=True)
    ip_address = models.TextField('IP адреса', blank=True)
    user_agent = models.TextField('User-Agent', blank=True)
    datetime = models.DateTimeField('Дата та час', auto_now_add=True)
    is_successful = models.BooleanField('Успішно')

    def __str__(self):
        return f'{self.username}'


    class Meta:
```

```
        verbose_name = 'Вхід'
        verbose_name_plural = 'Журнал входу'
        ordering = ['-id']

    @classmethod
    def create(cls, request) -> 'LoginLog':
        username = request.POST.get('username')
        if len(username) > 145:
            username = username[:145] + '...'
        log = LoginLog(
            username=username,
            is_successful=request.user.is_authenticated,
            user_agent=request.headers.get('User-Agent', ''),
        )
        if request.user.is_authenticated:
            log.user = request.user
        log.ip_address = cls.get_ip_from_request(request)
        log.save()
        return log

    @staticmethod
    def get_ip_from_request(request):
        forwarded = request.META.get('HTTP_X_FORWARDED_FOR', '')
        if forwarded:
            return forwarded.split(',')[0].strip()
        return request.META.get('REMOTE_ADDR', '')



models.py
---------------
from django.db import models
from django.contrib.auth import get_user_model

User = get_user_model()


class District(models.Model):
    name = models.CharField(verbose_name='Район', max_length=80, unique=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Район'
        verbose_name_plural = 'Райони'


class Settlement(models.Model):
    name = models.CharField(verbose_name='Населений пункт', max_length=80)
```

```
    district = models.ForeignKey(District, on_delete=models.CASCADE, related_name='settlement', verbose_name='Район')

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Населений пункт'
        verbose_name_plural = 'Населені пункти'


class ProviderType(models.Model):
    name = models.CharField(verbose_name='Назва', max_length=100, default='', blank=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Тип провайдера'
        verbose_name_plural = 'Типи провайдерів'


class CritCategories(models.Model):
    name = models.CharField(verbose_name='Назва', max_length=200)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['id']
        verbose_name = 'Категорія критичності'
        verbose_name_plural = 'Категорії критичності'


class ImplLevel(models.Model):
    name = models.CharField(verbose_name='Назва', max_length=220)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['id']
        verbose_name = 'Впровадження рівня кіберзахисту'
        verbose_name_plural = 'Впровадження рівнів кіберзахисту'


class Provider(models.Model):
    name = models.CharField(verbose_name='Назва', max_length=200)
    edrpou = models.CharField(verbose_name='ЄДРПОУ', max_length=30)
    created_at = models.DateTimeField(verbose_name='Дата створення', auto_now_add=True)
```

```
    district = models.ForeignKey(District, on_delete=models.CASCADE, related_name='provider', verbose_name='Район')
    settlement = models.ForeignKey(Settlement, on_delete=models.CASCADE, related_name='provider',
                                   verbose_name='Населений пункт')
    street = models.CharField(verbose_name='Вулиця', max_length=100)
    house = models.CharField(verbose_name='Будинок', max_length=8)
    prov_type = models.ForeignKey(ProviderType, on_delete=models.CASCADE, related_name='provider',
                                  verbose_name='Тип провайдера')
    ciso = models.TextField(verbose_name='Керівник ІТ-безпеки', blank=True, default='')

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Провайдер'
        verbose_name_plural = 'Провайдери'


class OKI(models.Model):
    name = models.CharField(verbose_name='Назва', max_length=250)
    created_at = models.DateTimeField(verbose_name='Дата створення', auto_now_add=True)
    updated_at = models.DateTimeField(verbose_name='Останні зміни', auto_now=True)
    district = models.ForeignKey(District, on_delete=models.CASCADE, related_name='oki', verbose_name='Район')
    settlement = models.ForeignKey(Settlement, on_delete=models.CASCADE,
                                   related_name='oki', verbose_name='Населений пункт')
    street = models.CharField(verbose_name='Вулиця', max_length=150)
    house = models.CharField(verbose_name='Будинок', max_length=10)
    provider = models.ForeignKey(Provider, on_delete=models.CASCADE, related_name='oki', verbose_name='Провайдер')
    crit_categories = models.ForeignKey(CritCategories, on_delete=models.CASCADE,
                                        related_name='oki', verbose_name='Категорія критичності')
    impl_level = models.ForeignKey(ImplLevel, on_delete=models.CASCADE, related_name='+',
                                   verbose_name='Рівень впровадження кіберзахисту')
    ciso = models.TextField(verbose_name='Керівник ІТ-безпеки', blank=True, default='')

    def __str__(self):
        return f'{self.name} ({self.provider}, {self.district}, {self.settlement}, {self.street} {self.house})'

    class Meta:
        verbose_name = "Об'єкт критичної інфраструктури"
        verbose_name_plural = "Об'єкти критичної інфраструктури"


class Analysis(models.Model):

    name = models.CharField(verbose_name='Назва', max_length=200)
    created_at = models.DateTimeField(verbose_name='Дата створення', auto_now_add=True)
```

```
    author = models.ForeignKey(User, on_delete=models.CASCADE, related_name='oki', verbose_name='Автор')
    oki = models.ForeignKey(OKI, on_delete=models.CASCADE, related_name='analysis', verbose_name="OKI")

    alarm = models.BooleanField(verbose_name='Сигналізація', default=False)
    video = models.BooleanField(verbose_name='Відеоспостереження', default=False)
    physical = models.BooleanField(verbose_name='Фізична охорона', default=False)
    access = models.BooleanField(verbose_name='Контроль доступу', default=False)
    fire = models.BooleanField(verbose_name='Протипожежний захист', default=False)
    power = models.BooleanField(verbose_name='Резервне енергозабезпечення', default=False)

    auth = models.BooleanField(verbose_name='Автентифікація користувачів', default=False)
    update = models.BooleanField(verbose_name='Регулярне оновлення', default=False)
    ips_ids = models.BooleanField(verbose_name=' IPS/IDS', default=False)
    mon = models.BooleanField(verbose_name='Моніторинг', default=False)
    info_sec = models.BooleanField(verbose_name='Захист інформації', default=False)
    backup = models.BooleanField(verbose_name='Резервне копіювання', default=False)

    score = models.PositiveIntegerField(verbose_name='Інтегральна оцінка безпеки', default=False)
    recommendation = models.TextField(verbose_name='Рекомендації', blank=True, default='')

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['-created_at']
        verbose_name = "Аналіз"
        verbose_name_plural = "Аналізи"


"""
WSGI config for system project.

It exposes the WSGI callable as a module-level variable named ``application``.

For more information on this file, see
https://docs.djangoproject.com/en/4.2/howto/deployment/wsgi/
"""

import os

from django.core.wsgi import get_wsgi_application

os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'system.settings')

application = get_wsgi_application()


[
{
  "model": "auth.group",
```

```
  "pk": 1,
  "fields": {
    "name": "ADMINISTRATOR",
    "permissions": []
  }
},
{
  "model": "auth.group",
  "pk": 2,
  "fields": {
    "name": "ANALYST",
    "permissions": []
  }
}
]
```

**Додаток В. Ілюстративний матеріал**

# ЗАХИЩЕНИЙ КОНСОЛІДОВАНИЙ ІНФОРМАЦІЙНИЙ РЕСУРС СИСТЕМНОГО АНАЛІЗУ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ РЕГІОНУ

Виконав: студент групи 1КІТС-22М Білоус В.М.

Науковий керівник: д.т.н., проф., професор каф.МБІС Яремчук Ю.Є.

## АКТУАЛЬНІСТЬ РОБОТИ

Забезпечення безпеки об'єктів критичної інфраструктури є надзвичайно актуальним, оскільки ці об'єкти є стратегічно важливими для держави та суспільства в цілому. Вони забезпечують життєдіяльність населення, економічну стійкість та безпеку країни.

## ОБ’ЄКТ ДОСЛІДЖЕННЯ

- Об’єктом дослідження є стан безпеки інформаційно-телекомунікаційної інфраструктури

## ПРЕДМЕТ ДОСЛІДЖЕННЯ

- Теоретичні і практичні заходи реалізації консолідованого ресурсу.

## НАУКОВА НОВИЗНА

- Вперше розроблено захищений консолідований інформаційний ресурс аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону, що надає можливість вирішення проблеми комплексного аналізу безпеки її критичних об’єктів для більш ефективного забезпечення безпеки

## КРИТИЧНА ІНФРАСТРУКТУРА

- Критична інфраструктура – це сукупність об'єктів, систем і процесів, які є життєво важливими для функціонування суспільства, національної економіки і безпеки країни.
- Вона включає у себе такі сектори, як енергетика, транспорт, водопостачання, комунікації, фінанси, охорона здоров'я, інформаційні технології, харчова промисловість, система захисту, комунальні послуги тощо.
- Критична інфраструктура є вразливою до природних катастроф, техногенних аварій, кібератак, терористичних актів та інших загроз. Захист і забезпечення безперебійної роботи критичної інфраструктури є важливим завданням для забезпечення безпеки суспільства та функціонування держави

## ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА ІНФРАСТРУКТУРА

- Телекомунікаційна мережа – це система передачі та обміну інформацією, що включає в себе різні засоби комунікації, такі як телефонні лінії, мобільні мережі, комп'ютерні мережі, супутникові системи зв'язку та інші.
- Інформаційно-телекомунікаційна інфраструктура (ITI) - це система, що включає в себе різноманітні технологічні засоби, мережі, програмні продукти, обладнання, послуги та людські ресурси, які необхідні для забезпечення передачі, обробки, зберігання та використання інформації у великому масштабі
- Основною метою інформаційно-телекомунікаційної інфраструктури є забезпечення надійного доступу до інформації та ефективного обміну даними між різними користувачами

## ОПЕРАТОРИ І ПРОВАЙДЕРИ

- Network Operator (мережевий оператор) – це компанія, яка забезпечує послуги зв'язку, такі як мобільна та фіксована телефонія, мобільний Інтернет, передача даних та інші послуги, шляхом управління і підтримки телекомунікаційних мереж. Мережевий оператор володіє, управляє та підтримує свою власну інфраструктуру, таку як базові станції, комутатори, маршрутизатори та інші обладнання, необхідні для надання послуг зв'язку своїм клієнтам
- Internet Service Providing, або професійне надання інтернет-сервісів, - це послуга, яка надається провайдерами для забезпечення доступу користувачів до Інтернету, тому ISP (постачальник сервісів Інтернету) надає підключення до Інтернету для домашніх користувачів, підприємств та інших організацій. ISP забезпечує підключення клієнтів до глобальної мережі Інтернет шляхом використання різних технологій і засобів передачі даних. Вони можуть мати свої власні мережі інфраструктури, які включають сервери, роутери, комутатори та інші обладнання для передачі інформації.

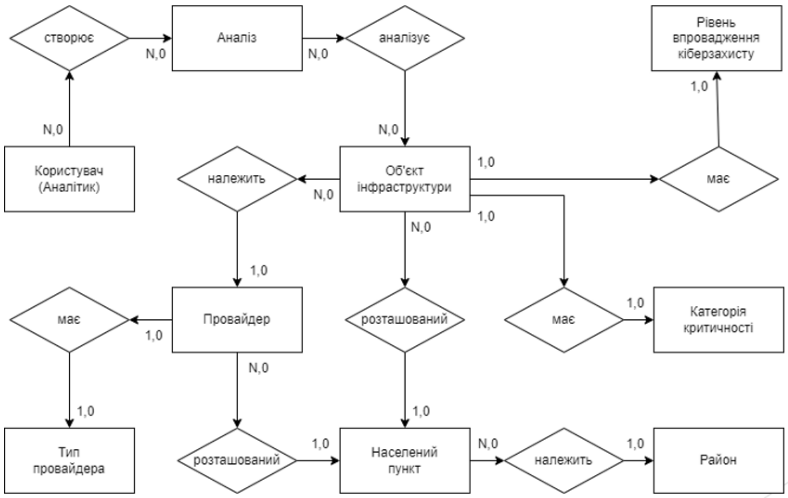
## РОЗРОБКА ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ

- розроблено основні модулі захищеного консолідованого інформаційного ресурсу аналізу безпеки
- досліджені і враховані особливості інформаційно-телекомунікаційної інфраструктури
- спроектована і розроблена база даних для функціонування інформаційного ресурсу, реалізовані звіти
- розроблено захист ресурсу

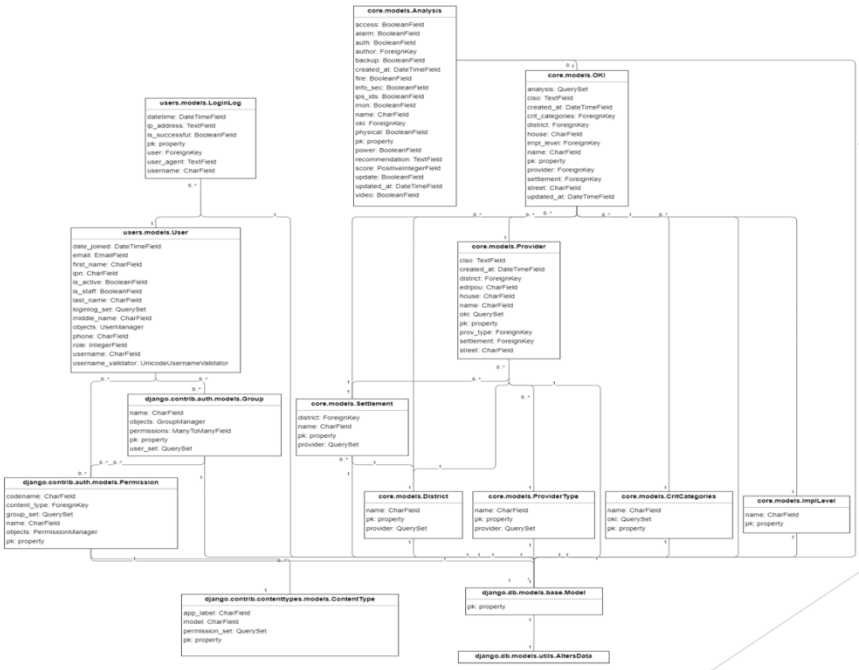
## УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ


Кібербезпека має цикл управління, що складається з 5 ключових функцій, які виконуються послідовно – ідентифікація ризиків, кіберзахист, виявлення інцидентів, реагування та відновлення нормального стану

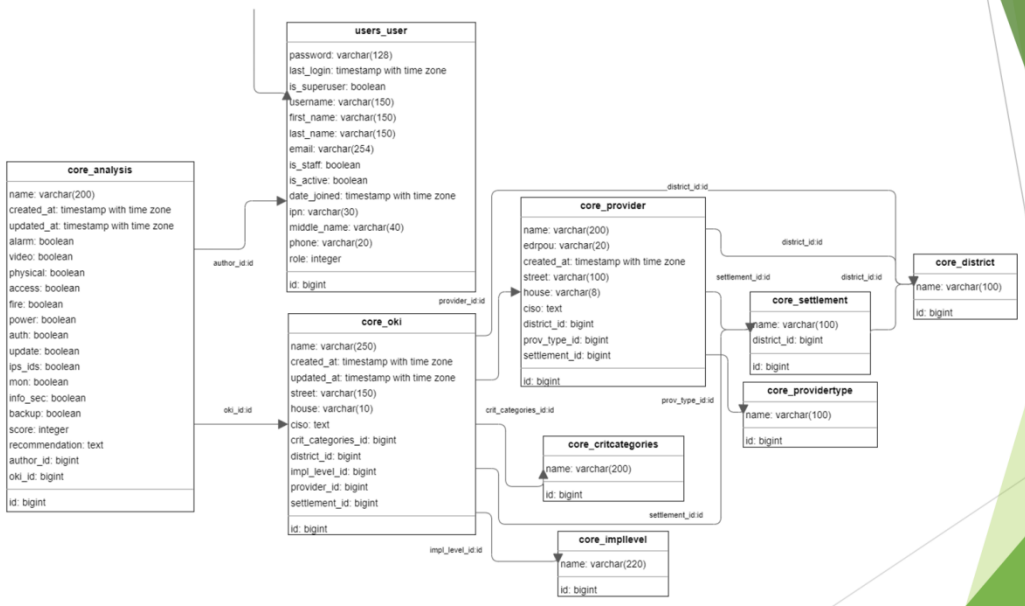
# ER-МОДЕЛЬ



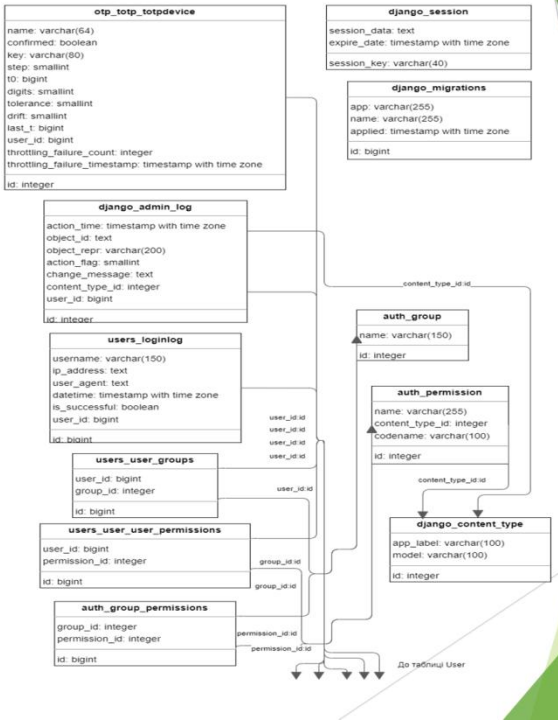

# UML-ДІАГРАМА КЛАСІВ



# БАЗА ДАНИХ (частина 1)




# БАЗА ДАНИХ (частина 2)



## ВИКОРИСТАНІ ТЕХНОЛОГІЇ


## ЗАХИСТ ІНФОРМАЦІЙНОГО РЕСУРСУ

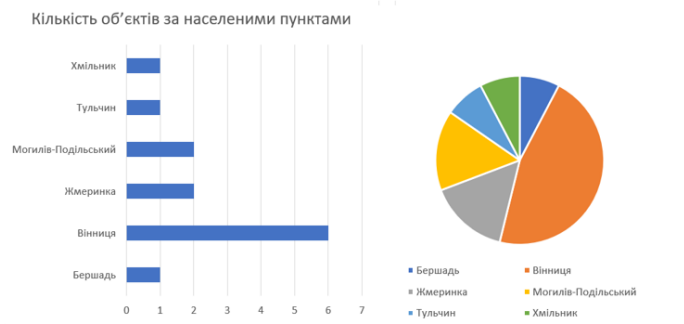
- **РОЗРОБЛЕНО**

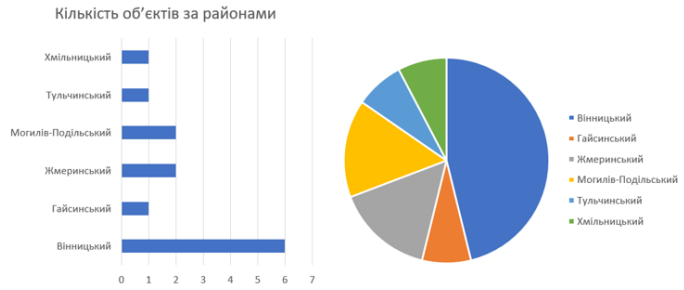
двофакторна автентифікація (2FA), розділення доступів користувачів згідно їх ролей, журнал дій користувача, журнал спроб входу в систему, окремий вхід на сайт для кожної ролі

- **ДОДАТКОВО НАЛАШТОВАНО**

захист від міжсайтових сценаріїв XSS (Cross site scripting), захист від підробки міжсайтового запиту CSRF (Cross-site request forgery), захист від SQL-ін'єкції, захист від клікджекінгу (Clickjacking), перевірка заголовка хосту (Host header check), політика реферерів (HTTP referer), політика відкриття між джерелами (Cross-origin opener policy), безпека сесії

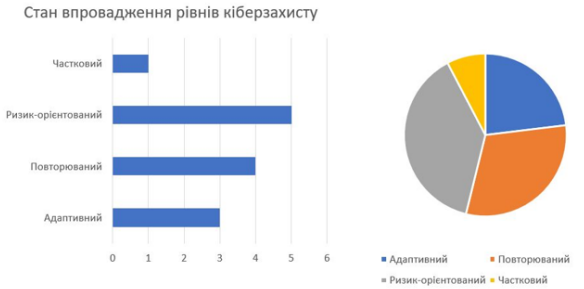
# АНАЛІТИЧНІ ЗВІТИ (1–2)



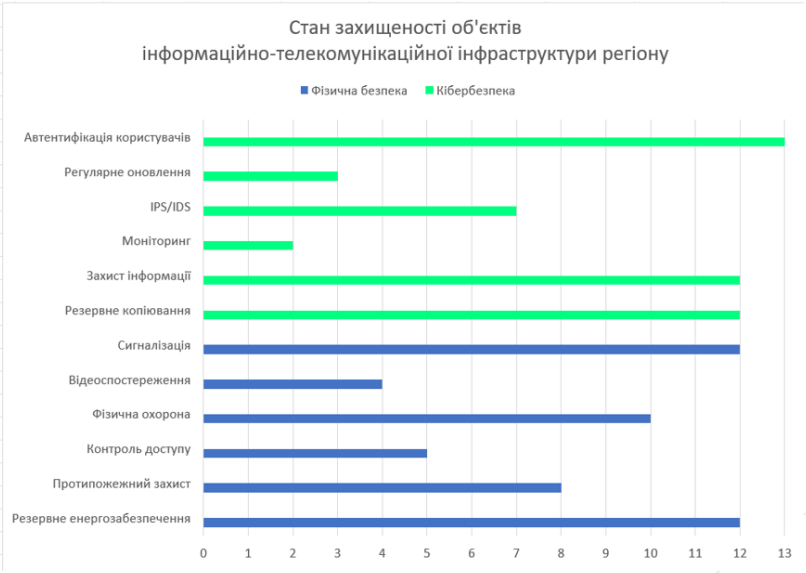

# АНАЛІТИЧНІ ЗВІТИ (3–4)


# АНАЛІТИЧНІ ЗВІТИ (5–6)

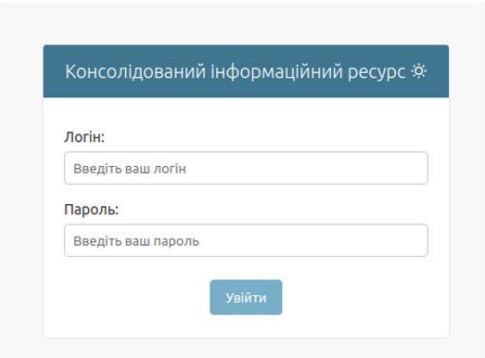


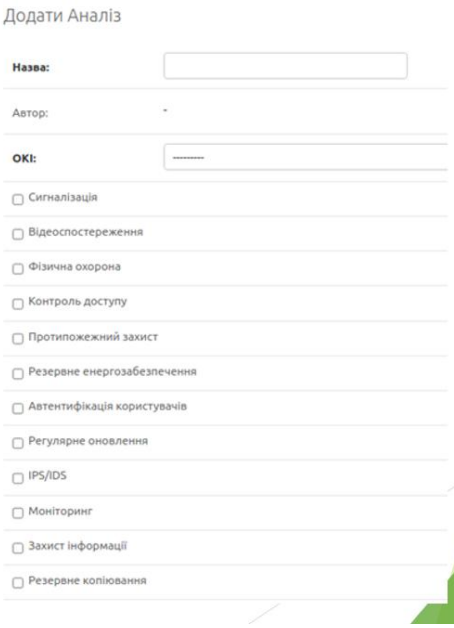


# АНАЛІТИЧНІ ЗВІТИ (7)



# ІНТЕРФЕЙС




# ВИСНОВКИ

Досліджено принципи та методи збору та обробки даних для системного аналізу, а також проаналізовано питання забезпечення безпеки інформаційних ресурсів.

Розглянуто вимоги законодавства щодо створення консолідованого інформаційного ресурсу для аналізу безпеки інформаційно-телекомунікаційної інфраструктури.

Розроблена архітектура інформаційного ресурсу та його функціонал, визначено сутності та їх взаємозв'язки.

Розроблено алгоритми обробки та аналізу безпеки об’єктів інформаційно-телекомунікаційної інфраструктури, проведено реалізацію бази даних та формування аналітичних звітів.

Магістерська робота успішно досягла своєї основної мети, представлена розробка захищеного консолідованого інформаційного ресурсу для системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону, яка дозволить аналізувати і покращувати безпеку важливих об’єктів, а також можливості для подальшого вдосконалення інформаційного ресурсу.

**ДЯКУЮ ЗА УВАГУ!**

## Додаток Г. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

**Показники звіту подібності Unicheck**

Оригінальність 98 % Схожість 2 %

Аналіз звіту подібності (відмітити потрібне):

**1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.**

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ (підпис) Коваль Н.П. (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) Білоус В.М. (прізвище, ініціали)

Керівник роботи _____ (підпис) Яремчук Ю.Є. (прізвище, ініціали)