**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Система кіберзахисту інформаційних ресурсів у сфері електронного уряду України

|  |  |
| --- | --- |
| **Автор:** | Ю.В. Кравчук |
| **Науковий керівник:** к.т.н., доц. | А.Б. Єлізаров |
| **Нормоконтролер:** асистент | С.В. Єгоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Кравчук Юлії Вячеславівни**

1. Тема: *Система кіберзахисту інформаційних ресурсів у сфері електронного уряду України* затверджена наказом ректора від «\_\_» \_\_\_\_\_\_ 20\_\_ № \_\_\_\_\_/ст*.*
2. Термін виконання з 14.10.2019р. по 09.02.2020р*.*
3. Вихідні дані: проаналізувати існуючі системи та методики аналізу і оцінки ризиків інформаційної безпеки; на основі аналізу виділити вхідні і вихідні параметри, завдяки яким можливо провести порівняння існуючих систем, виявлення їх переваг і недоліків; розробити методику, алгоритм та програмне забезпечення системи аналізу і оцінки ризиків.
4. Зміст пояснювальної записки: аналіз існуючих систем та методик аналізу і оцінки ризиків інформаційної безпеки; розробка методики системи аналізу та оцінки ризиків на основі нечіткої логіки; розробка програмного забезпечення запропонованої системи, верифікація отриманих результатів.

Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Завдання | Термін виконання | Примітки |
| 1 | Уточнення поставки завдання | 15.10.2019 |  |
| 2 | Аналіз літературних джерел | 17.10.2019 – 24.10.2019 |  |
| 3 | Ознайомлення з основними поняттями та цілями електронного уряду | 25.10.2019 |  |
| 4 | Аналіз методик кіберзахисту сфери національної безпеки | 26.10.2019 – 02.11.2019 |  |
| 5 | Збір інформації про існуючі постанови та закони про покращення рівня безпеки інформаційних ресурсів на державних підприємствах | 03.11.2019 – 19.11.2019 |  |
| 6 | Розробка архітектури програмної компоненти | 20.11.2019 – 30.11.2019 |  |
| 7 | Розробка сервісів для системи | 01.11.2019 – 19.01.2020 |  |
| 8 | Тестування роботи системи | 20.01.2020 – 29.01.2020 |  |
| 9 | Оформлення і друк пояснювальної записки | 30.01.2020 |  |
| 10 | Оформлення презентації | 01.02.2020 |  |
| 11 | Отримання рецензії від опонента | 02.02.2020 |  |
| 12 | Підготовка до захисту в ЕК | 03.02.2020 - 04.02.2020 |  |

Дата видачі завдання: \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_р.

Керівник дипломної роботи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання*:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (П.І.Б)

**УДК**

**РЕФЕРАТ**

Пояснювальна записка до дипломної роботи «Аудит інформаційної безпеки підприємства»: 97 сторінок, 6 рисунки, 5 таблиць, 24 літературних джерел.

Ключові слова: СИСТЕМА, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, НАЦІОНАЛЬНА БЕЗПЕКА, ВИМОГИ, ПРОГРАМНА КОМПОНЕНТА, ВИПРОБУВАННЯ СИСТЕМИ.

Об’єкт дослідження: є державна система кіберзахисту інформації від кібератак.

Предмет дослідження: є програмна компонента системи інформаційної безпеки.

Мета дипломної роботистворити програмну компоненту системи кіберзахисту інформаційних ресурсів електронного уряду, для забезпечення найповнішого зосередження інформації щодо кіберінцидентів, накопичення, керування цими знаннями, а також попередження та запобігання кібератак.

Значущість виконаної роботи та висновки: в результаті виконання роботи, було розроблено програмну компоненту, яка є частиною системи кіберзахисту інформаційних ресурсів у сфері електронного уряду.

Результати роботи у вигляді програми дають основу для подальшого інтегрування в систему національної безпеки.

Рекомендації щодо використання результатів: в роботі було розглянуто вимоги до системи інформаційної системи, на основі яких було створено програму для підвищення рівня кіберзахисту державних підприємств.

Система може бути технологічно інтегрованою із зовнішніми системами, включаючи системи обробки та зберігання даних та Ситуаційні центри кібербезпеки.

[**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ** 6](#_Toc30452554)

[**ВСТУП** 7](#_Toc30452555)

[**РОЗДІЛ 1 – ПРИНЦИПИ ПОБУДОВИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРЗАХИСТУ** 10](#_Toc30452556)

[**1.1 Аналіз існуючих автоматизованих систем в сфері ІБ** 10](#_Toc30452557)

[1.1.1 Основні поняття 10](#_Toc30452558)

[1.1.2 Поняття інформаційно-аналітичних систем 12](#_Toc30452559)

[**1.2 Передумови для поліпшення національної системи кіберзахисту** 22](#_Toc30452560)

[**1.3 Програмний продукт як основна складова інформаційно-аналітичної системи** 27](#_Toc30452561)

[**Висновки до розділу** 38](#_Toc30452562)

[**РОЗДІЛ 2 – РОЗРОБКА ПРОГРАМНОЇ КОМПОНЕНТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ** 40](#_Toc30452563)

[**2.1 Вимоги до модулів та функцій системи** 40](#_Toc30452564)

[2.1.1 Вимоги до функціонування системи 40](#_Toc30452565)

[2.1.2 Вимоги, які необхідно виконати для сумісності з зовнішніми системами 42](#_Toc30452566)

[2.1.3 Режими функціонування 44](#_Toc30452567)

[2.1.4 Вимоги до надійності 47](#_Toc30452568)

[2.1.5 Вимоги до захисту інформації від несанкціонованого доступу 54](#_Toc30452569)

[**2.2 Архітектура Системи (логічна компонента)** 57](#_Toc30452570)

[**2.3 Інтерфейс та опис функцій розділів Систем (зовнішня компонента)** 64](#_Toc30452571)

[**2.4 Функціональна структура Системи (внутрішня компонента)** 77](#_Toc30452572)

[**Висновки до розділу** 81](#_Toc30452573)

[**РОЗДІЛ 3 – ДОСЛІДЖЕННЯ ПРОГРАМНОЇ КОМПОНЕНТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ** 82](#_Toc30452574)

[**3.1 Випробування системи** 82](#_Toc30452575)

[**3.2 Сумісність Системи із зовнішніми системами** 90](#_Toc30452576)

[**Висновки до розділу** 92](#_Toc30452577)

[**ВИСНОВОК** 93](#_Toc30452578)

[**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ** 94](#_Toc30452579)

[**Додаток А** 97](#_Toc30452580)

**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ**

API Application Programming Interface (програмний інтерфейс додатку)

CERT Computer Emergency Response Team (команда

реагування на комп’ютерні надзвичайні події)

EDR Endpoint Detection and Response (реагування на рівні

кінцевих точок)

MPLS Multiprotocol Label Switching (багатопротокольна

комутація по мітках)

SOC Security Operations Center (центр оперативного реагування)

TI Threat Intelligence

ІТС Інформаційно-телекомунікаційна система

ПЗ Програмне забезпечення

СД Спеціальні дані

ТВ Технічні вимоги

БД База даних

ОС Операційна система

СОД Система обробки даних

НСКЗ Національна система конфіденційного зв’язку

# **ВСТУП**

**Оцінка сучасного стану проблеми.** Глобальна інформатизація в даний час активно управляє існуванням і життєдіяльністю держав світової спільноти, інформаційні технології застосовуються при вирішенні завдань забезпечення національної, військової, економічної безпеки та ін. Разом з тим, одним з фундаментальних наслідків глобальної інформатизації державних і військових структур стало виникнення принципово нового середовища протиборства конкуруючих держав — кіберпростору, яке не є географічним в загальноприйнятому сенсі того слова, але, однак (одначе), в повній мірі є міжнародним.

І якщо сьогодні між провідними у військовому та економічному відношенні світовими державами склався так чи інакше певний паритет в області застосування звичайних озброєнь і зброї масового ураження, в міжнародному праві зафіксовані основні принципи взаємовідносин цих держав в рамках таких просторів, як наземне, морське, повітряне, космічне, то питання про міждержавний паритет і взаєминах в кіберпросторі на даний час продовжує залишатися відкритим.

У процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, в провідних закордонний державах розробляються нові засоби і методи активного впливу на інформаційну інфраструктуру потенційних супротивників, створюються різні спеціалізовані кібернетичні центри та підрозділи управління і командування, основним завданням яких є захист державних і військових інформаційних інфраструктур.

**Актуальність роботи.** У сучасних умовах цілком справедливе твердження про те, що війни XXI столітті будуть кібернетичними за своєю основною суттю. Отже, для будь-якої держави безпеку в кіберпросторі (кібербезпека) ставати гострою і специфічною проблемою в забезпеченні своєї національної безпеки і захисту своїх інтересів.

**Метою є** створення програмної компоненти системи кіберзахисту інформаційних ресурсів електронного уряду, для забезпечення найповнішого зосередження інформації щодо кіберінцидентів, накопичення, керування цими знаннями, а також попередження та запобігання кібератак

Для досягнення поставленої мети поставлені такі задачі:

* Аналіз існуючих систем та підходів до їх реалізації
* Визначення способу для удосконалення існуючої системи
* Визначення вимог та задач, які система має реалізувати
* Формування архітектури програмної компоненти
* Розробка основних модулів та їх тестування
* Випробування готової програмної системи

**Галузь застосування**. Розроблена система та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності інформаційних ресурсів у сфері електронного уряду України.

**Об’єктом дослідження** є державна система кіберзахисту інформації від кібератак.

**Предметом дослідження** є програмна компонента системи інформаційної безпеки.

**Новизна одержаних результатів полягає в наступному:**

В роботі було удосконалено систему кіберзахисту інформаційних ресурсів у сфері електронного уряду України завдяки програмній компоненті, яку було розроблено відповідно поставлених вимог, використовуючи мову програмування PHP 7 та середовище розробки для JetBrains PHPStorm.

**Практичне значення отриманих результатів:**

* розроблено програмний продукт для централізованого збору, обробки та накопичення інформації про кіберінциденти.
* дооснащенно організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти.

**Апробація.** Основні положення роботи доповідалися та обговорювалися на таких конференціях:

* Основні положення роботи доповідалися та обговорювалися на XV Міжнародній науково-практичній конференції «Наукові горизонти – 2019», том 15. («Scientific Horizons – 2019», volume 15) – 30.09.2019 – 7.10.2019.

# **РОЗДІЛ 1 – ПРИНЦИПИ ПОБУДОВИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРЗАХИСТУ**

# **1.1 Аналіз існуючих автоматизованих систем в сфері ІБ**

## 1.1.1 Основні поняття

Виконуючи роботу, першим етапом необхідно визначити основні терміни та поняття в сфері кіберзахисту.

*Система* – порядок, зумовлений правильним, планомірним розташуванням і взаємним зв’язком частин чого-небудь; сукупність яких-небудь елементів, одиниць, частин, об’єднуваних за спільною ознакою, призначенням.

*Кіберзахист* (англ. Cyber Defence) — сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Кіберзахист покликаний допомагати у розробці та керувати стратегіями, необхідними для протидії шкідливим атакам або загрозам. Широкий спектр різних видів діяльності залучається до кібербезпеки для захисту визначеного суб'єкта, а також для швидкого реагування на кібератаки. Це може включати зменшення привабливості визначеного суб'єкта для можливих зловмисників, розуміння критичних місць та конфіденційної інформації, запровадження запобіжних заходів для забезпечення протидії кібератакам, можливості виявлення кібератак та реагування. Кіберзахист також передбачає проведення технічного аналізу для визначення шляхів і областей, які можуть атакувати зловмисники.

Впровадження системи кіберзахисту передбачено законом “Про основні засади забезпечення кібербезпеки України”.

Електронний уряд — це модель державного управління, яка заснована на використанні сучасних інформаційних та комунікаційних технологій з метою підвищення ефективності та прозорості влади, а також встановлення суспільного контролю над нею. Є однією із базових складових електронного урядування.

Агентство з питань електронного урядування України, на ряду з іншими Міністерствами та Державними службами, виступили з позиції зацікавлених органів у створенні системи кіберзахисту інформаційних ресурсів.

Така система дозволить підвищити рівень кіберзахисту об’єктів критичної інформаційної інфраструктури держави шляхом створення механізму взаємодії суб'єктів забезпечення кібербезпеки під час попередження, виявлення, припинення та усуненні наслідків кібератак та кіберінцидентів.

Серед загальних проблем, з якими зіткнулись країни під час впровадження електронного урядування були різні підходи щодо вирішення різних труднощів. Так, наприклад, для більшості країн однією з головних проблем було забезпечення сумісності різнорідних інформаційних систем, що створювались в різні роки, за різними принципами, на різних технологічних платформах. Системи електронного урядування працюють на основі інформаційних систем, що побудовані на корпоративних комп’ютерних мережах. Тому, на функціонування систем електронного урядування мають вплив також проблеми, характерні для корпоративних структур. З цими проблемами доводиться стикатися як фахівцям у галузі технічного обслуговування, так і службам інформаційної безпеки у сфері публічного управління.

Таким чином, під час створення та використання системи електронного урядування потрібне розв’язання важливих проблем як з її технічного обслуговування, так і щодо інформаційної безпеки. [2]

## 1.1.2 Поняття інформаційно-аналітичних систем

Більшість сучасних автоматизованих систем складаються з таких компонентів:

- Платформа, на якій функціонують інші компоненти системи, що містить апаратуру (залізо) і системне ПО.

- Дані, з якими працює система. Складаються з СУБД і баз даних.

- Додатки, що реалізують бізнес-логіку по роботі з даними системою. Складаються з компонентів бізнес-логіки, призначеного для користувача інтерфейсу, допоміжних компонентів (фреймворк) і сервера додатків, який забезпечує зберігання і доступ до компонентів програми.

- Бізнес-процеси, які являють собою сценарії роботи користувачів з системою.

Тому, інтеграція інформаційних систем полягає в інтеграції одного або декількох компонентів інтегрованих інформаційних систем (об'єктів інтеграції):

Цілями інтеграції платформ є:

- забезпечення можливості взаємодії між додатками, що працюють на різних програмно-апаратних платформах (наприклад, між додатками, що працюють на серверах Windows, Solaris, Linux і ін;

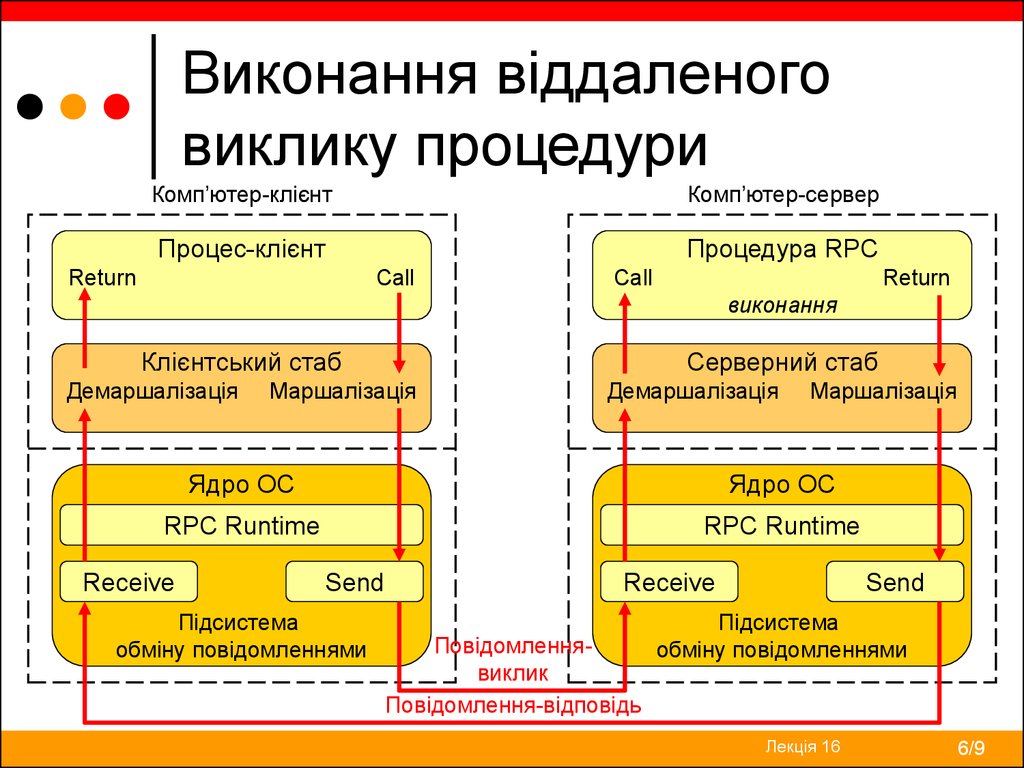
- забезпечення можливості роботи додатків, розроблених для однієї програмно-апаратної платформи, на інших програмно-апаратних платформах (наприклад, додатків Windows на платформах Linux, Solaris і ін.). Існує кілька підходів, спрямованих на досягнення цих цілей:

- віддалений виклик процедур (RPC, CORBA, DCOM, Web-сервіси);

- ПО проміжного шару (Microsoft.Net, Java Runtime);

- віртуалізація.

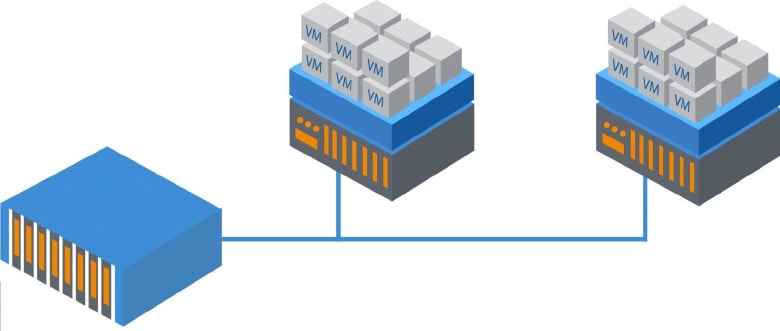
Технології віддаленого виклику процедур (в широкому сенсі під процедурою розуміється деяка функціональність програми) дозволяють опублікувати процедуру і забезпечити можливість її виклику (передачі входять параметрів і отримання вихідних результатів) для додатків, що працюють на інших платформах. Елементами таких технологій зазвичай є: загальний для всіх платформ мова опису інтерфейсів процедур (IDL, WSDL), «адаптер» (перехідник) процедури, який транслює зовнішні виклики у внутрішні і передає результати назад і менеджери, що відповідають за доставку запитів і результатів між платформами в мережі (брокери). Прикладами технологій віддаленого виклику процедур є: RPC, CORBA, DCOM, Web-сервіси.



Концепція програмного забезпечення проміжного шару (framework, середовище виконання, віртуальна машина) складається в розробці прикладного ПЗ не з використанням сервісів конкретної операційної системи (наприклад, Windows API), а з використанням сервісів ПО проміжного шару. Розробниками ПЗ проміжного шару створюються її реалізації під різні операційні системи, які транслюють виклики відповідних функцій фрейворка в виклики відповідної операційної системи. Типовим прикладом є технологія Java Runtime Environment. Додатки, розроблені для цієї технології працюють на будь-яких програмно-апаратних платформах. Без жодних допрацювань самих додатків. Аналогічні можливості надаються серед Microsoft .Net Framework.



Цікавою і сучасною концепцією є «віртуалізація». До інтеграції платформ вона має відношення остільки, оскільки дозволяє істотно спростити використання різних платформ і, відповідно, використання систем, що вимагають для свого функціонування наявності конкретних платформ. На кожному з таких «віртуальних» серверів можуть бути розгорнуті відповідні системи, які будуть доступні одночасно.



За визначенням інформаційна система працює з даними. У переважній більшості випадків система має в своєму складі базу даних для їх зберігання. Інтеграція на рівні даних передбачає спільне використання даних різних систем. Інтеграція даних може виявитися простіше, ніж інтеграція додатків, тому що промислові СУБД, в яких зазвичай зберігають дані інформаційні системи, мають розвинені можливості програмного доступу до даних з інших додатків. Самі додатки при цьому можуть мати вельми обмежені можливості програмного (поза власним призначеного для користувача інтерфейсу) використання своєї функціональності зовнішніми системами.

Підходи до інтеграції даних:

- універсальний доступ до даних;

- сховища даних.

Технології універсального доступу до даних дозволяють забезпечити однаковий доступ до даних різних СУБД. Посередником для роботи з конкретною СУБД в даному випадку є драйвер для відповідної СУБД. Це дозволяє абстрагуватися від специфіки конкретних СУБД і легко здійснювати інтеграцію даних, що зберігаються в різних СУБД. Найбільш поширені технології цього класу: ODBC, JDBC.

Інтеграція даних включає об'єднання даних, що знаходяться в різних джерелах, і надання даних користувачам в уніфікованому вигляді. Роль інтеграції даних зростає, коли збільшується обсяг і необхідність спільного використання даних.

Системи інтеграції даних можуть забезпечувати інтеграцію даних на фізичному, логічному і семантичному рівні. Інтеграція даних на фізичному рівні з теоретичної точки зору є найбільш простим завданням і зводиться до конверсії даних з різних джерел в необхідний єдиний формат їх фізичного представлення.

Інтеграція даних на логічному рівні передбачає можливість доступу до даних, що містяться в різних джерелах, в термінах єдиної глобальної схеми, яка описує їх спільне подання з урахуванням структурних і, можливо, поведінкових (при використанні об'єктних моделей) властивостей даних. Семантичні властивості даних при цьому не враховуються. Підтримку єдиного уявлення даних з урахуванням їх семантичних властивостей в контексті єдиної онтології предметної області забезпечує інтеграція даних на семантичному рівні.

Процесу інтеграції перешкоджає неоднорідність джерел даних, відповідно до рівня інтеграції. Так, при інтеграції на фізичному рівні в джерелах даних можуть використовуватися різні формати файлів. На логічному рівні інтеграції може мати місце неоднорідність використовуваних моделей даних для різних джерел або розрізняються схеми даних, хоча використовується одна і та ж модель даних. Одні джерела можуть бути веб-сайтами, а інші - об'єктними базами даних і т. Д. При інтеграції на семантичному рівні різних джерел даних можуть відповідати різні онтології. Наприклад, можливий випадок, коли кожен з джерел представляє інформаційні ресурси, що моделюють певну частину предметної області, якому відповідав би своя понятійна система, і ці фрагменти перетинаються.

При створенні системи інтеграції виникає ряд завдань, склад яких залежить від вимог до неї та використовуваного підходу. До них, зокрема, відносяться:

Архітектури систем інтеграції:

а) Консолідація. У разі консолідації дані витягуються з джерел, і поміщаються в Сховище даних. Процес заповнення Сховища складається з трьох фаз - витяг, перетворення, завантаження (Extract, Transformation, Loading - ETL). У багатьох випадках саме ETL розуміють під терміном «інтеграція даних». Ще одна поширена технологія консолідації даних - управління змістом корпорації (enterprise content management, скор. ECM). Більшість рішень ECM спрямовані на консолідацію і управління неструктурованими даними, такими як документи, звіти і web-сторінки.

б) Федералізація. У федеративних БД фізичного переміщення даних не відбувається: дані залишаються у власників, доступ до них здійснюється при необхідності (при виконанні запиту). Спочатку федеративні БД припускали створення в кожному з n вузлів n-1 фрагментів коду, що дозволяє звертатися до будь-якого іншого вузла.

в) Поширення даних. Додатки поширення даних здійснюють копіювання даних з одного місця в інше. Ці програми зазвичай працюють в оперативному режимі і виробляють переміщення даних до місць призначення, тобто залежать від певних подій. Оновлення в первинній системі можуть передаватися в кінцеву систему синхронно або асинхронно. Синхронна передача вимагає, щоб поновлення в обох системах відбувалися під час однієї і тієї ж фізичної транзакції. Незалежно від використовуваного типу синхронізації, метод поширення гарантує доставлення даних в систему призначення. Така гарантія - це ключовий відмітна ознака поширення даних. більшість технологій синхронного поширення даних підтримують двосторонній обмін даними між первинними і кінцевими системами. Прикладами технологій, що підтримують поширення даних, є інтеграція корпоративних додатків (Enterprise application integration ) і тиражування корпоративних даних (Enterprise data replication, скор. EDR).

г) Сервісний підхід. Сервісно-орієнтована архітектура (Service Oriented Architecture), успішно застосовується при інтеграції додатків, може бути застосована і при інтеграції даних. Дані також залишаються у власників і навіть місцеперебування даних невідомо. При запиті відбувається звернення до певних сервісів, які пов'язані з джерелами, де знаходиться інформація і її конкретну адресу.

Незалежно від обраних технології та методу інтеграції даних, залишаються питання, пов'язані з їх змістовною інтерпретацією і відмінностями в поданні одних і тих самих речей. Тому доводиться вирішувати невідповідність схем даних і невідповідність самих даних.

Типи невідповідності схем даних:

- Конфлікти неоднорідності (використовуються різні моделі даних для різних джерел);

- Конфлікти іменування (в різних схемах використовується різна термінологія, що призводить до омонімії і синонімії в іменуванні);

- Семантичні конфлікти (обрані різні рівні абстракції для моделювання подібних сутностей реального світу);

- Структурні конфлікти (одні й ті ж сутності представляються в різних джерелах різними структурами даних)

Інтеграція на рівні додатків має на увазі використання готових функцій додатків іншими додатками. Варто згадати такі підходи до інтеграції додатків:

- інтерфейси прикладного програмування;

- обмін повідомленнями (Корпоративна шина сервісів);

- сервісно-орієнтована архітектура;

- інтеграція призначених для користувача інтерфейсів.

Інтерфейс прикладного програмування конкретної системи вдає із себе «опублікований» функціонал цієї системи, який може бути використаний ззовні. Функціонал може публікуватися у вигляді набору функцій (приклад - Windows API) або у вигляді об'єктної моделі (об'єкти з властивостями і методами, приклад - об'єктні моделі додатків Microsoft Office).

Сервісно-орієнтована архітектура (SOA) є сучасною парадигмою. Вона є логічним продовженням концепції Web-сервісів, яка складається в публікації функціональних блоків будь-якої програми в вигляді, що дозволяє отримати до них доступ іншим додатком через Web. Web (протокол HTTP) в даному випадку привабливий з огляду на можливості його використання і, відповідно, використання опублікованих в Web додатків на будь-яких програмно-апаратних платформах. Web-сервіс - невелика програмна надбудова над функціоналом додатки, що перетворює виклики, й виходила через Web у внутрішні виклики функцій програми і повертає результати назад. [27]

Існує велика кількість програмних продуктів для інтеграції систем: комерційний і безкоштовних, з закритими кодами і Open Source, дорогих і дешевих, з різною функціональністю, розрахованих на різний масштаб бізнесу користувачів. Можна виділити наступні класи продуктів для інтеграції систем:

- реалізують ідеологію SOA;

- реалізують ідеологію Messaging (проміжне ПО);

- корпоративні шини сервісів;

- кошти інтеграції на рівні бізнес-процесів (BPEL, Business Process Execution Language);

- кошти інтеграції даних.

Серйозні продукти для інтеграції корпоративних додатків від солідних вендорів охоплюють компоненти відразу декількох класів з перерахованих вище. У цьому огляді обмежимося продуктами від трьох вендорів: Microsoft, Oracle та IBM.

Microsoft BizTalk Server. BizTalk Server являє собою програмний продукт для інтеграції додатків і бізнес-процесів. Архітектура BizTalk Server, заснована на ідеології обміну повідомленнями між додатками. Центральною частиною системи є механізм обміну повідомленнями (Engine), який складається з двох частин:

- Messaging - транспортний рівень (приймання, зберігання та надсилання повідомлень між додатками), підключення до обміну різних систем, що функціонують на різних платформах, використання облікових записів для підключення до систем;

- Orchestration - правила (логіка) обробки повідомлень. Наприклад, за допомогою візуального дизайнера можна визначити алгоритм, відповідно до якого, отримавши повідомлення від термінала необхідно створити повідомлення для CRM-системи та бухгалтерської системи з метою подальшої обробки факту продажу.

Microsoft SQL Server. Загальновідома СУБД Microsoft SQL Server є також прикладом платформи для інтеграції даних. Функції інтеграції реалізуються в MS SQL Server наступними компонентами: Integration Services і Analysis Services. Integration Services є ETL-інструментом, що дозволяє:

- Зібрати дані з різних джерел (наприклад, реляційних БД, текстових файлів, RSS-каналів в Інтернеті, веб-сервісів і ін.);

- Перетворити їх з вихідних форматів в необхідні з використанням проміжних сховищ або без них. Правила перетворення і консолідації задаються розробниками сховища;

- Помістити результат в інформаційне сховище, в якому вони стають доступними споживачам інтегрованої інформації. Analysis Services підтримує процес інтеграції даних на наступних етапах, а саме:

- Створення OLAP-сховищ, в яке стікаються дані з різних джерел в процесі інтеграції, і зберігання багатовимірних даних;

- Забезпечення доступу до OLAP-даних, виконання багатовимірних запитів. Типовий приклад - робота з даними за допомогою Pivot Table.

- Інтелектуальний автоматизований аналіз даних (Data Mining).

Oracle Business Activity Monitoring - панель управління (dashboard) інтегрованими бізнес-процесами. Дозволяє переглядати різні показники бізнес-процесів (наприклад, KPI), сервісів і їх компонентів в «одному вікні».

Oracle Business Rules - засіб опису бізнес-правил і політик, використовуваних в інтегрованих бізнес-процесах.

IBM WebSphere. IBM WebSphere - це middleware від IBM, аналог Oracle Fusion. У складі IBM WebSphere є продукти, що забезпечують інтеграцію систем в парадигмі SOA (по аналогії з Oracle SOA Suite). Склад і функціонал продуктів схожий на аналогічне ПО інших вендорів:

WebSphere Business Modeler - засіб візуального опису інтегрувальних бізнес-процесів.

WebSphere Process Server - хостинг і виконання бізнес-процесів.

WebSphere Integration Developer - середовище розробки сервісних компонентів.

WebSphere Business Monitor - інструмент моніторингу бізнес-процесів.

Інтеграція даних включає об'єднання даних, що знаходяться в різних джерелах, і надання даних користувачам в уніфікованому вигляді. Цей процес стає істотним як у комерційних завданнях (коли двом схожим компаніям необхідно об'єднати їх бази даних), так і в наукових (комбінування результатів дослідження з різних інформаційних репозитаріїв). Роль інтеграції даних зростає, коли збільшується обсяг і необхідність спільного використання даних.

# **1.2 Передумови для поліпшення національної системи кіберзахисту**

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру.

Війна в кіберпросторі спричиняє нові кіберзагрози. Кіберзагрози – це наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим інтересам людини та громадянина, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем

Загрози інформаційній безпеці: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом

Дооснащення НСКЗ покликано забезпечити виконання таких завдань, окреслених в Стратегії кібербезпеки України:

1. впровадження організаційно-технічної моделі національної системи кібербезпеки, швидкого реагування на кібератаки та кіберінциденти;

2. розгортання єдиної системи ситуаційних центрів профільних державних органів сектору безпеки та оборони на основі безпечної інформаційної інфраструктури;

3. розробка нових методів запобігання та поширення кібератак, кібер-інцидентів;

4. розробка вимог (правил, вказівок) щодо безпечного користування Інтернетом та надання електронних послуг державними органами;

5. підвищення обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведення відповідних тренінгів, навчань;

6. проведення навчань з надзвичайних ситуацій та інцидентів у кіберпросторі;

7. розвиток мережі комп’ютерних команд реагування на надзвичайні ситуації;

8. створення системи для своєчасного виявлення, запобігання та нейтралізації кіберзагроз;

9. створення умов для впровадження в Україні сучасних технологій кіберзахисту;

10. налагодження співпраці між суб’єктами забезпечення кіберзахисту критичної інфраструктури, розвиток державно-приватного партнерства щодо запобігання кіберзагрозам, реагування на кібератаки та кібер-інциденти, усунення їх наслідків;

11. розробка та впровадження механізму обміну інформацією між органами державної влади, приватним сектором та громадянами щодо загроз критичній інформаційній інфраструктурі;

12. періодичний огляд національної системи кібербезпеки, розробка галузевих показників кібербезпеки;

13. розробка та впровадження протоколів спільних дій, включаючи обмін інформацією в реальному часі, суб'єкти кібербезпеки при виявленні кібератак та кібер-інцидентів;

14. сприяння розвитку системи реагування на надзвичайні ситуації для комп’ютерних надзвичайних ситуацій;

15. розробка та координація досліджень з питань кібербезпеки та кіберзахисту для потреб національної безпеки та оборони;

16. посилення здатності суб'єктів боротьби з кібертероризмом протидіяти кібер-атакам на державні електронні інформаційні ресурси, засоби критичної інфраструктури, а також розвідувальну та підривну діяльність іноземних спецслужб, організацій, груп та осіб проти кіберпростору тощо. [25]

**Нормативне обґрунтування**

Нормативно-правовою базою для дооснащення НСКЗ є:

* Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016;
* Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» від 13 лютого 2017 року №32/2017;
* Указ Президента України «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32» від 30 серпня 2017 року № 254/2017;
* Розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» від 10 березня 2017 року № 155-р.

Законодавчою та нормативною базою функціонування НСКЗ є:

* Закон України "Про інформацію" (із змінами і доповненнями) від 2 жовтня 1992 року № 2657-XII;
* Закон України "Про телекомунікації" (із змінами і доповненнями) від 18 листопада 2003 року № 1280-15;
* Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (зі змінами і доповненнями) від 5 липня 1994 року № 80/94-ВР;
* Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 22 лютого 2006 року № 3475-IV;
* Положення про технічний захист інформації в Україні. Затверджено Указом Президента від 27.09.1999 р. №1229/99;
* Порядок підключення до глобальних мереж передачі даних, затверджений постановою Кабінету Міністрів України від 12.04.2002 № 522;
* Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, затверджений постановою Кабінету Міністрів України від 16.11.2002 № 1772;
* Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.06 № 373;
* Правила надання та отримання телекомунікаційних послуг, затверджені постановою Кабінету Міністрів України від 11.04.2012 № 295;
* Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 03.09.14 № 411;
* Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563;
* ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
* ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
* НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;;
* НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу;
* РД 50-34.698-90. Автоматизировані системи. Вимоги до змісту документів.

Розпорядчою базою функціонування НСКЗ є:

* Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв’язку від 10.06.2008 № 94;
* Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв’язку від 02.12.2014 № 660;
* Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті, затверджений наказом Адміністрації Держспецзв’язку від 15.01.2016  № 20. [25]

**Науково-технічне та технічне обґрунтування**

На базі Державного центру кіберзахисту і протидії кіберзагрозам Державної служби спеціального зв’язку та захисту інформації України функціонують підрозділи, що забезпечують:

1. отримання інформації про кіберінциденти, розслідування та реагування на них (команда реагування на комп’ютерні надзвичайні події (CERT-UA));
2. захищене підключення інформаційно-телекомунікаційних систем органів державної влади (далі – ІТС ОДВ) до ресурсів мережі Інтернет (захищений вузол Інтернет-доступу (ЗВІД)).

Нинішні технічні, методичні та організаційні ресурси Державного центру з кібербезпеки та кіберзагроз не повністю відповідають потребам, необхідним для ефективного вирішення завдань Стратегії кібербезпеки Державного секретаріату. Таким чином, для забезпечення нового рівня захисту від сучасних кіберзагроз, запобігання кібератакам та кіберінцидентам необхідно запровадити:

● система централізованого збору, обробки та накопичення інформації про кіберінциденти;

● система кореляції, аналізу та зберігання структурованих та неструктурованих журналів даних функціонування інформаційних інфраструктур та інформаційної безпеки;

● система обміну інформацією про кіберзагрози з суб'єктами кібербезпеки та сторонніми постачальниками інтелектуального контенту для систем кіберзахисту;

● система накопичення та управління знаннями про кіберінциденти;

● система тестування кіберзагроз та зловмисних програм.

# **1.3 Програмний продукт як основна складова інформаційно-аналітичної системи**

Програмна компонента складається з:

1. Онлайн-кабінету користувачів Системи у складі:

1.1. Система відстеження запитів клієнтів;

1.2. Система звітності та статистики;

1.3. Система інформування користувачів;

1.4. Система мережевих інструментів;

1.5. Система верифікації мереж.

2. Система збору та нормалізації даних з наступних джерел:

2.1. Модуль пасивного моніторингу;

2.2. Модуль активного моніторингу.

3. Система накопичення даних моніторингу.

4. Система обробки та візуалізації даних.

5. Модуль інтеграції із зовнішніми системами (API).

**Принципи побудови та взаємодії із зовнішніми системами**

- врахування існуючих компонентів системи кіберзахисту (ЗВІД);

- забезпечення технологічної сумісності з існуючими системами кіберзахисту;

- здійснення контролю зовнішніх ІТС;

- масштабування (підключення ОДВ та об’єктів критичної інфраструктури);

- наявність технічних та організаційних інтерфейсів взаємодії з міжнародними та національними системами.

**Вимоги до Онлайн-кабінету користувачів системи**

Онлайн-кабінет уявляє собою веб-сайт, що після авторизації надає доступ користувачам до інформації про вразливості або підозрілу активність в їх мережах.

Онлайн-кабінет має містити наступні розділи та функціональні блоки (назва розділів для різних типів користувачів може відрізнятись):

1. Управління користувачами, у тому числі:

1.1. Блок реєстрації користувачів;

1.2. Налаштування профілю користувача.

2. Управління організаціями.

3. Налаштування мереж.

4. Верифікація мереж.

5. Управління сенсорами активного моніторингу.

6. Відстеження запитів клієнтів (ticket-система).

7. Звітність та статистика.

8. Інформування користувачів.

8.1. Внутрішня система повідомлень.

8.2. Зовнішнє інформування.

9. Мережеві інструменти.

10. Новини.

11. Часті запитання (FAQ).

12. Завантаження.

13. Обробка та візуалізація даних (див. розділ «Система обробки та візуалізації даних»).

14. Wiki.

**Управління користувачами**

Система повинна мати не менше чотирьох типів користувачів та наступний функціонал для них, а саме:

1. Користувач приватного сектору:

1.1. Налаштування власного профілю користувача;

1.2. Налаштування власної мережі (подача заявки на верифікацію, перегляд та управління власними мережами). Занесення відомостей про власні мережі шляхом відображення їх на карті;

1.3. Створення запиту клієнта та подальша робота зі власними запитами (без можливості пріоритезації запитів);

1.4. Звітність та статистика у межах своєї мережі;

1.5. Внутрішня система повідомлень;

1.6. Зовнішнє інформування (опціонально);

1.7. Мережеві інструменти (з обмеженнями);

1.8. Новини (з обмеженнями);

1.9. Часті запитання;

1.10. Завантаження (з обмеженнями).

2. Користувач ОДВ (додатково до користувача приватного сектору):

2.1. Запит на встановлення активного сенсору;

2.2. Перегляд загальних даних профілю інших користувачів, що відносяться до даної ОДВ;

2.3. Зовнішнє інформування, доступ до мережевих інструментів, новин та завантажень – без обмежень;

2.4. Перегляд карти зі своїми мережами;

2.5. Створення запиту клієнта та подальша робота зі своїми запитами (з обмеженою можливостю пріоритезації запитів).

3. Адміністратор (додатково до користувача ОДВ)

3.1. Здійснює керування користувачами приватного сектору та ОДВ;

3.2. Здійснює верифікацію користувачів ОДВ;

3.3. Можливість ручної верифікації мереж користувачів;

3.4. Доступ до звітів та статистики для усіх мереж користувачів (в тому числі в реальному часі);

3.5. Створення запиту клієнта (для зовнішніх джерел із повідомленнями про інциденти) та подальша робота з запитами (з можливостю пріоритезації запитів);

3.6. Опрацювання запитів клієнтів системи (користувачів приватного сектору, ОДВ, запитів, зроблених іншими Адміністраторами);

3.7. Перегляд статистики відповідей на запити клієнтів (в межах запитів, що були опрацьовані Адміністратором);

3.8. Перегляд карти усіх мереж;

3.9. Перегляд дій користувачів системи (користувачів ОДВ та приватного сектору).

4. Адміністратор найвищого рівня (додатково до Адміністратора)

4.1. Здійснює керування усіма типами користувачів Системи;

4.2. Здійснює керування організаціями системи;

4.3. Перегляд статистики відповідей на запити клієнтів (повністю);

4.4. Перегляд усіх дій Адміністраторів Системи.

**Блок реєстрації користувачів**

- Система повинна здійснювати логічну перевірку заповнених відомостей (наприклад, перевірка правильності формату введення телефону або електронної поштової скриньки);

- Система повинна здійснювати перевірку зареєстрованої електронної поштової скриньки шляхом надсилання унікального посилання для підтвердження реєстрації скриньки;

- Система повинна дозволяти реєстрацію з однаковим номером телефону тільки у тому випадку, якщо такого номеру телефону немає ні в кого з підтверджених, активних користувачів;

- Система повинна мати механізм нагадування паролю із використанням вказаної адреси електронної поштової скриньки;

- Опціонально: нагадування паролю через СМС;

- Використання двохфакторної аутентифікації;

- Система повинна бути стійкою до брутфорсу;

- Оповіщення про реєстрацію та інші дії користувачів в онлайн кабінеті адміністратора сайту через внутрішню систему повідомлень;

- Надсилання електронних листів до користувачів системи:

- Під час реєстрації та після її успішного завершення;

- Зміни особистих даних (наприклад зміна паролю);

- Зміни статусу двохфакторної аутентифікації;

- Заборона реєстрації по ІР-адресам;

- Користувач отримує доступ до розділів Системи (крім даних свого профілю) тільки після проходження верифікації зі сторони Адміністратора;

Налаштування профілю користувача:

Розділ дає можливість користувачеві відредагувати свої контактні дані:

- Логін;

- ПІБ;

- Пароль;

- Поштова скринька (зі зміною тільки після верифікації нової скриньки);

- Увімкнення двохфакторної аутентифікації;

Система повинна надсилати відповідні повідомлення електронною поштою після зміни користувачем даних свого профілю.

**Управління організаціями**

Система повинна мати перелік Організацій (установ) що відносяться до ОДВ, об’єктів критичної інфраструктури, тощо. Включення організації до переліку відбувається за письмовим поданням до Адміністратора системи.

Редагування списку організацій здійснюється в ручному режимі Супер Адміністратором Системи.

Перелік організацій має бути із зазначенням їх структурних одиниць.

**Налаштування мереж**

- Розділ надає можливість користувачеві ввести інформацію (ІР-адреси) про свою мережу та відмітити її місцезнаходження на карті для подальшої візуалізації. За вказаною інформацією користувач у майбутньому отримуватиме звіти;

- Користувач повинен мати можливість вводити назви для кожної своєї мережі;

- Додатково користувач може додати для відстежування домен сайту (також із проходженням верифікації на право управління ресурсом);

- Користувач може видаляти свої мережі;

- Користувач може мати більше однієї мережі. Після додавання, кожна окрема мережа проходить окрему верифікацію на право управління ресурсом.

**Верифікація мереж**

Верифікація мереж проходить у спосіб додавання спеціального html-файлу за прикладом верифікації прав власності на домен в інструментах Google. Для верифікації домену також може використовуватись спеціальний мета-тег на сторінці веб-сайту.

Для ситуацій, коли верифікація вказаними методами неможлива, у системі повинна бути передбачено підтвердження права управління мережею вручну Адміністратором.

Історія проходження верифікації мережі вноситься до відповідних записів в лог-файли системи та відсилання відповідного повідомлення Адміністратору найвищого рівня системи.

Після проходження верифікації Користувач отримує доступ до даних, які стосуються його мережі, інцидентів, повідомлень, тощо.

**Управління сенсорами активного моніторингу**

Розділ дає можливість продивлятися спрацювання свого сенсору (декількох сенсорів) у реальному часі.

Користувач ОДВ може продивлятися деталі роботи сенсору тільки в межах своїх мереж, якщо такий сенсор в нього встановлений. Адміністратор системи має також узагальнену інформацію щодо роботи усіх сенсорів у системі.

Користувач системи повинен мати можливість переглядати:

- Статус роботи сенсора;

- Карта з розміщенням і статусами сенсорів;

- Графічне подання мережевого трафіку;

- Детальна інформація про склад мережевого трафіку за вказаний період;

- Перегляд виявлених джерел компрометації, їхніх типів та ін.

**Відстеження запитів клієнтів (ticket-система)**

Система відстеження запитів клієнтів повинна мати повний базовий функціонал   
ticket-системи що дозволяє:

- Налаштовувати правила адресації запитів до Адміністраторів системи в т.ч. переадресації від користувача до користувача, налаштувань чергових Адміністраторів тощо;

- Система повинна дозволяти встановлювати максимально можливий час відповіді на запит в залежності від пріоритету, тематики та типу загрози в запиті. Після спливання такого терміну Адміністратор найвищого рівня повинен отримувати повідомлення про те, що запит залишився без розгляду зі сторони Адміністратору (-ів);

- Мати набори фільтрів та сортування для зручної роботи Адміністраторів з переліком запитів4

- Мати зручний вигляд списку запитів з відображенням статусу, пріоритету, наявності коментарів, файлів, виконавців запиту, часом реагування на запит, тощо;

- Інформування користувачів системи (внутрішнє і зовнішнє) про нові запити, отримання відповідей у запиті, зміна статусу і т.д;

- Статистика запитів

Бізнес-процеси запитів (послідовність зміни статусів та ін.) формуються на етапі проектування системи.

Запити повинні містити параметри:

- Джерело запиту (ПІБ користувача, або вказання типу зовнішнього каналу, якщо запит прийшов за телефоном або в усній формі);

- Організація, від якої надійшов запит;

- Тематика;

- Тип загрози;

- Пріоритет;

- Додаткові нотатки.

**Звітність та статистика**

Розділ дає можливість отримувати та завантажувати звіти, які формуються системою пасивного та активного моніторингу.

Користувач повинен мати можливість:

- отримувати обрані дані в онлайн-кабінеті;

- вказувати період для формування звіту, тип загроз та інші критерії, що наявні у модулях активного та пасивного моніторингу;

- завантажувати дані з можливістю вибору по фільтрам в форматах .txt .pdf .doc;

- отримувати на поштову адресу або/та внутрішню поштову систему обрані дані із обраною періодичністю.

**Інформування користувачів**

Внутрішня система повідомлень.

Система повинна мати внутрішню систему повідомлень щодо:

- Появи важливих новин від Адміністратора;

- Зміни статусу, пріоритету запиту, створеного користувачем;

- Зміни статусу верифікації користувача, його мереж, запуску чи припинення функціонування сенсорів, що встановлені в його установі;

- Появи інцидентів у його мережі (та реакції сенсору на інцидент у разі, якщо є налаштовані політики автоматичної реакції сенсорів на інцидент);

- Внутрішньої взаємодії між користувачами системи в рамках своєї організації.

**Зовнішнє інформування**

Вимоги до зовнішньої системи інформування аналогічні до внутрішньої системи повідомлень, з використанням e-mail:

Мережеві інструменти;

Мережеві інструменти (калькулятор підмережі, whois, nslookup, тощо);

Новини;

Стрічка новин;

Часті запитання;

Перелік корисних матеріалів та відповідей на часті питання від CERT-UA у вигляді списку статей та окремих сторінок для кожного матеріалу.

**Завантаження**

Перелік ПЗ, що використовується для роботи сенсорів (у разі, якщо користувач має встановлений сенсор) та інших корисних утиліт та ПЗ.

**Система збору та нормалізації даних**

Система повинна задовольняти такі загальні вимоги:

- Збір даних з різних типів каналів пасивного моніторингу (наприклад, потоки даних у реальному часі);

- Нормалізація даних для приведення в єдиний вид, що використовується системою у роботі та для подальшого збереження;

- Можливість додавання даних про загрози та інциденти вручну Адміністратором Системи;

- Можливість створення власного потоку нормалізованих даних для передавання у зовнішні системи;

**Модуль пасивного моніторингу НСК**

- Обробка інформації, яка надходить до CERT-UA з різних джерел у вигляді електронних листів, звітів, мережевого потоку, звернень,

- Обробка отриманої інформації, формування звітів

- Перелік джерел з яких надходить інформація:

- Bitsight;

- Arbor;

- Shadowserver;

- Spamhaus;

- BotnetTracker;

- Дані, внесені Адміністратором Системи, про загрози та інциденти через окремий модуль

- Система пасивного моніторингу повинна зберігати та обробляти у реальному часі потік не менше ніж 400 MB/s

- Розгортання модуля пасивного моніторингу на віртуальному сервері з ОС Ubuntu

**Модуль активного моніторингу**

- Розробка/модернізація програмного засобу для моніторингу/блокування мережевих загроз (IDS/IPS);

- Створення інсталяційного пакету для розгортання системи моніторингу (сенсору) в інформаційно-телекомунікаційних системах на сервері з ОС Ubuntu, та налаштування VPN клієнту з заданими параметрами;

- Експорт даних з сенсорів до серверу баз даних;

- Розділ з візуалізацією виявлених загроз в онлайн-кабінеті.

**Система накопичення даних моніторингу**

Усі наявні дані про кіберзагрози та інциденти, джерела компрометації та інша інформація, що надходить з джерел активного та пасивного моніторингу повинні зберігатись у Системі не менше трьох років

Дані моніторингу повинні бути зарезервовані із використанням зовнішніх ресурсів НСК.

**Система обробки та візуалізації даних**

Модуль візуалізації аналітичних даних - веб-додаток, який є динамічно оновлюваною картою України. Дані для візуалізації беруться з БД аналітичної інформації.

Веб-додаток складається з двох частин:

1. Карта України на якій показано локації державних органів та їх ІР-адреси. Якщо в БД є скомпрометована ІР-адреса, яка належить державному органу маркер державного органу стає червоним. При натисканні на маркер показується інформація щодо вразливостей на конкретних ІР-адресах. Якщо ІР-адреси державного органу немає в БД скомпрометованих, то маркер стає зеленим.

2. Карта усіх скомпрометованих ІР-адрес України. Карта України, на якій показано усі скомпрометовані ІР-адреси, які знаходяться в БД CERT-UA за деякий період часу, наприклад за останні півроку. ІР-адреси помічаються червоними маркерами, якщо вони заражені шкідливим ПЗ, жовтими якщо інші вразливості. При натиску на маркер виводиться список типів вразливостей обраної ІР-адреси. Для реалізації використовується БД скомпрометованих ІР-адрес, БД геолокацій ІР та БД ІТС державних органів.

Модуль карти повинен відображати додаткові дані щодо кількості скомпрометованих адрес за день, тиждень, місяць.

**Модуль інтеграції із зовнішніми системами (API)**

АРІ повинно реалізувати можливість інтеграції з зовнішніми системами для запровадження доступу до даних Системи:

- Звітність та статистика.

- Інформування про наявні кіберзагрози та кіберінциденти.

- Рекомендації щодо попередження кіберінцидентів.

- Інформація про стан запитів користувача.

Можливість доступу до API здійснюється тільки через особистий ключ, що створюється для кожного користувача окремо і може бути отримано в Онлайн-Кабінеті.

**Загальні вимоги**

- Обов’язкова робота за протоколом HTTPS;

- Повне логування дій усіма користувачами системи;

- Система повинна бути побудована із урахуванням розподіленого розташування апаратних складових Системи;

- Система повинна бути побудованою із урахуванням можливого розширення апаратної частини для забезпечення високої продуктивності;

- Система повинна мати усі необхідні ліцензії для функціонування із попередньо визначеними навантаженнями на мережу, серверне обладнання та кількість облікових записів Адміністраторів, користувачів ОДВ та користувачів приватного сектору;

- Система повинна передбачати можливість додавання мобільної версії та мобільного додатку у майбутньому. [2]

# **Висновки до розділу**

У першому розділі було розглянуто питання про інформаційну безпеку, яку за сферою застосування необхідно розглядати в контексті безпеки держави, організації та особистості.

Для реалізації законодавчих, нормативно-правових та нормативних актів з інформаційної безпеки повинна створюватися комплексна система захисту інформації.

Захист інформації охоплює сукупність методів і засобів,

забезпечують цілісність, конфіденційність і доступність інформації по

умовах впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до нанесення шкоди власникам і користувачам інформації.

Концепція технічного захисту інформації в Україні є складовою

забезпечення національної безпеки України і визначає основи державної політики в сфері захисту інформації інженерно-технічними

засобами.

Стратегія захисту інформації визначає основу для побудови

комплексу заходів щодо інформаційної безпеки, передбачаючи необхідні, конкретні засоби захисту, які є найбільш дієвими з точки зору

наявних інформаційних, фінансових і людських ресурсів.

# **РОЗДІЛ 2 – РОЗРОБКА ПРОГРАМНОЇ КОМПОНЕНТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ**

# **2.1 Вимоги до модулів та функцій системи**

## 2.1.1 Вимоги до функціонування системи

Для нормального функціонування системи, я виділила основні принципи, на яких вона має базуватися:

незалежність

відкритість

модульність

масштабованість

керованість і конфігурування

системність

персоналізація

єдність графічного представлення

захищеність інформації

* *незалежність* – архітектура системи повинна забезпечити технологічну нейтральність і адаптивність від конкретних реалізацій і технічних рішень інформаційних систем органів державної влади та на об’єктах критичної інформаційної інфраструктури, що забезпечує максимальну інтероперабельність, як за спектром рішень, так і в часі, при зміні версій програмного забезпечення та появі нових технологій;
* *відкритість* – система повинна використовувати загальнодоступні й специфіковані рішення, протоколи й інтерфейси, що має забезпечувати інтеграцію створюваних рішень як між собою, так й із зовнішніми інформаційними системами;
* *модульність* – система повинна бути побудована з використанням модульної архітектури, що передбачає реалізацію основних функцій як окремих модулів, що забезпечують можливість їх незалежної модифікації. Збій у роботі одного з модулів не повинен приводити до повного припинення функціонування системи в цілому;
* *масштабованість* – архітектура системи повинна дозволяти збільшувати продуктивність систем, обсяги збереженої й оброблюваної інформації без тривалої зупинки роботи й значної модифікації програмного коду;
* *керованість і конфігурування* – має бути забезпечене керування системою на всіх рівнях її архітектури: на рівні інфраструктури, на функціональному рівні, на рівні представлення даних;
* *системність* – усі взаємозалежні програмні модулі системи мають використовувати єдину методологію, і відповідати єдиним принципам взаємодії, надійності й керування;
* *персоналізація* – надання інформації користувачам повинне здійснюватися з урахуванням персональних налаштувань користувачів;
* *єдність графічного представлення* – при проектуванні й розробці користувацьких інтерфейсів повинні використовуватися загальні принципи графічного представлення інформації й організації доступу користувачів до функціональних можливостей і сервісів системи;
* *захищеність інформації* – мають бути передбачені механізми й заходи із забезпечення захисту службової інформації обмеженого доступу.

Виконуючи роботу, я обрала метод представлення системи як веб-сайт, який після авторизації буде надавати доступ користувачам до інформації про вразливості або підозрілу активність в їх мережах.

Система буде складатися з розділів, що будуть пов’язані між собою, а саме:

управління користувачами;

управління організаціями;

налаштування мереж;

верифікація мереж;

управління сенсорами активного моніторингу;

звітність та статистика;

інформування користувачів:

мережеві інструменти;

новини;

часті запитання (FAQ);

завантаження;

обробка та візуалізація даних;

Wiki.

Обладнання та програмне забезпечення Системи повинно забезпечувати тісну інтеграцію її елементів та підсистем, містити відкриті і/або спеціалізовані інтерфейси взаємодії та обміну даними. В результаті, обладнання та програмне забезпечення Системи має інтегруватись в існуючу інфраструктуру кіберзахисту кінцевого користувача та інших програмно-апаратних комплексів.

## 2.1.2 Вимоги, які необхідно виконати для сумісності з зовнішніми системами

В процесі функціонування Система буде технологічно інтегрованою із зовнішніми системами (зовнішніми структурними елементами):

* Системи обробки та зберігання даних (єдиний основний та резервний захищений дата-центр збереження інформації і відомостей державних інформаційних ресурсів);
* Захищені вузли Інтернет-доступу;
* Ситуаційні центри суб’єктів забезпечення кібербезпеки.

Зовнішні структурні елементи повинні взаємодіяти і/або мати можливість тісної технологічної інтеграції з Системою та її внутрішніми структурними елементами за допомогою відкритих та спеціалізованих інтерфейсів, протоколів та методів із застосуванням технологій забезпечення конфіденційності та цілісності даних, що передаються.

Архітектура Системи повинна передбачати інтерфейси взаємодії з ІТС підприємств і організацій будь-якої форми власності;

Спеціальні дані (далі – СД) ідентифікують загрози, вразливості, інциденти в ІТС. Джерелами таких даних є зовнішні структурні елементи Системи.

Спеціальні дані всередині і зовні Системи повинні передаватися за допомогою відкритих і/або стандартизованих (відповідно до RFC – Request for Comments) в індустрії технологій, протоколів та портів (наприклад, syslog, netflow, http/https тощо).

Підключення до підсистем буде здійснюватися за допомогою маршрутизаторів доступу або спеціалізованих шлюзів як з відкритих (публічних), так і з закритих (відомчих) мереж передачі даних. У випадках використання публічних мереж (зокрема Інтернет) необхідно передбачити організацію захищених з’єднань для забезпечення конфіденційності та цілісності СД. Захист такої інформації при передачі через незахищене середовище має здійснюватися у відповідності до вимог у сфері захисту інформації.

В якості потоків СД із зовнішніх джерел буде підключений спеціальний інформаційних потік Bitsight.

Розроблена Система буде здійснювати накопичення і обробку щонайменше таких категорій СД:

* дані про ІР-адреси вузлів і кінцевих точок, скомпрометованих уразливостями або уражених шкідливим програмним забезпеченням, та їх належність до фізичних або юридичних осіб;
* дані про ІР-адреси вузлів і кінцевих точок, на які здійснювались кібератаки та їх належність до фізичних або юридичних осіб;
* дані про ІР-адреси вузлів і кінцевих точок, що здійснюють розсилку шкідливого ПЗ, містять фішингові ресурси, та їх належність до фізичних або юридичних осіб.

В якості джерел СД для Системи можуть в майбутньому виступати:

* пасивні сенсори користувачів системи;
* підсистема збору телеметрії з ІТС користувачів системи;
* підсистема виявлення і реагування на атаки на рівні кінцевих точок;
* потоки СД із зовнішніх джерел «Threat Intelligence» (далі – TI);
* системи забезпечення кіберзахисту. [29]

## 2.1.3 Режими функціонування

Щодо режимів роботи Системи, я вирішила виділити:

штатний режим функціонування;

сервісний режим функціонування;

аварійний режим функціонування.

*Штатний режим функціонування Системи* – режим, в якому всі компоненти Системи виконують всі свої основні функції. В штатному режимі функціонування Система  повинна забезпечувати:

* роботу всіх користувачів в режимі - 24 годин на день, 7 днів на тиждень, 365 днів на рік (24х7х365);
* виконання всіх своїх основних функцій.

*Сервісний режим функціонування Системи* – режим, в якому повинна забезпечувати можливість проведення наступних робіт:

* планове технічне обслуговування;
* установку оновлених версій програмного забезпечення;
* модернізацію апаратно-програмного комплексу.

В даному режимі Система або її компоненти стають недоступними для певних груп користувачів. Загальний час проведення сервісних робіт не повинна перевищувати 12 годин в місяць від загального часу роботи в штатному режимі.

*Аварійний режим функціонування Системи* – режим, який характеризується відмовою одного або декількох компонентів програмного і (або) технічного забезпечення, зниженням якості її функціонування та інших аварійних ситуаціях. У разі переходу Системи в передаварійний режим необхідно забезпечити:

* завершення роботи всіх програмних компонентів, зі збереженням даних;
* проведення резервного копіювання баз даних.

Для забезпечення високої надійності функціонування Системи як в цілому, так і її окремих компонентів повинно забезпечуватися ведення в електронній формі журналів інцидентів, а також графіків і журналів проведення профілактичних робіт.

Програмне забезпечення Системи буде надавати зручний інтерфейс для можливості перегляду діагностичних подій, моніторингу процесу функціонування його компонентів.

Система буде передбачати можливість для:

* розширення та підвищення продуктивності апаратної частини;
* розширення функціональних можливостей компонентів в ході її поетапного розвитку та їх масштабування;

Експлуатація підсистем команди розрахована на використання штатними посадовими особами відповідних підрозділів центру кіберзахисту та протидії кіберзагрозам.

***Вимоги до кваліфікації персоналу***

Основні задачі з керування Системою будуть покладені на адміністратора (або декількох адміністраторів), а використання Системи призначені для відповідних операторів та аналітиків. Через специфіку роботи, для всіх цих спеціалістів є свої вимоги, описані мною нижче.

*До кваліфікації оператора, аналітика, оглядача звітів юридичних осіб*, ІТС які підключені і/або слугують джерелами інформації Системи висуваються наступні кваліфікаційні вимоги:

* бути досвідченим користувачем ПК
* мати навички по роботі в локальній обчислювальній мережі;
* мати навички використання додатків, призначених для роботи в мережі Інтернет (веб-браузер, поштовий клієнт);
* володіти навичками і вміннями роботи з пакетом Microsoft Office або аналогічними програмами по створенню електронних документів:
* мати досвід використання і настройки параметрів браузера, клієнта електронної пошти і програми для передачі файлів по протоколу FTP.

*До кваліфікації адміністратора юридичних осіб*, ІТС які підключені і/або слугують джерелами інформації Системи висуваються наступні кваліфікаційні вимоги:

* Операційна система сервера БД і додатків:
  + встановлення та налаштування системи;
  + управління користувачами;
  + призначення прав доступу;
  + управління локальною політикою безпеки.
* Сервер додатків:
  + створення та налаштування віртуального WWW сервера;
  + створення та налаштування віртуальних директорій;
  + настройка різних способів авторизації, дозвіл / заборона анонімного доступу до сервера;
  + вміння аналізувати лог-файли сервера.
* Веб-програмування:
  + знання базових HTML тегів.
* Мережеві протоколи:
  + TCP / IP. Способи адресації і маршрутизації пакетів;
  + DNS. Методи розпізнавання імен в мережі Інтернет.  Розуміння MX запису;
  + HTTP 1.1. Установка з'єднання з сервером, параметр "Host".
  + HTTPS / SSL.
* СУБД:
  + встановлення та налаштування;
  + створення, видалення, відновлення баз даних;
  + виконання SQL-скриптів і запитів до бази;
  + настройка авторизації;
  + створення користувачів, установка прав доступу до баз і таблиць.

## 2.1.4 Вимоги до надійності

Наступні вимоги я сформувала, опираючись на державні стандарти ІБ та безпеки на підприємстві.

Рівень надійності компонентів Системи повинен забезпечуватися за рахунок:

* застосування загальносистемного та спеціалізованого програмного забезпечення, які відповідають класу вирішуваних завдань;
* проведенням комплексу заходів налагодження, пошуку й виключення помилок;
* відновлення роботи програмного забезпечення Системи після відмови у разі виникнення програмного збою;
* веденням журналів системних повідомлень і помилок по програмним компонентам для наступного аналізу;
* контролю вхідної та вихідної інформації;
* розмежування прав доступу до програмного комплексу;
* ведення протоколів (архівів) дій користувачів;
* періодичного створення резервних копій.

Система повинна зберігати працездатність і забезпечувати відновлення своїх функцій при виникненні наступних позаштатних ситуацій:

* при збоях в системі електропостачання апаратної частини, що призводять до перезавантаження ОС, відновлення програми має відбуватися після перезапуску ОС і запуску виконуваного файлу системи;
* при помилках в роботі апаратних засобів (крім носіїв даних і програм), відновлення функцій програмних компонентів, при цьому, покладається на ОС;
* при помилках, пов'язаних з програмним забезпеченням (ОС і драйвери пристроїв), відновлення працездатності покладається на ОС.

Система повинна бути стійкою до хибних дій користувачів - помилки у діях персоналу не повинні приводити до збоїв (відмов) у роботі компонентів системи, всі дані, що вводяться користувачем, повинні перевірятися на формальну коректність. [19]

***Вимоги до ергономіки та технічної естетики***

Взаємодія користувачів з прикладним програмним забезпеченням, що входить до складу Системи має здійснюватися за допомогою графічного інтерфейсу користувача, який повинен бути зрозумілим і зручним, не повинен бути перевантажений графічними елементами і повинен забезпечувати швидке відображення екранних форм. Навігаційні елементи та компоненти інтерактивної взаємодії повинні бути виконані у зручній для користувача формі.

У частині зовнішнього оформлення графічний інтерфейс користувача повинен відповідати наступним вимогам:

* реалізацію в графічному віконному режимі за стандартами, прийнятими для програмних компонентів, що функціонують під керуванням графічної багатозадачної операційної системи;
* єдиному стилю оформлення екранних форм для всіх програмних компонентів; з однаковим розташуванням основних елементів керування та навігації;
* повинне бути забезпечена наявність україномовного інтерфейсу користувача;
* розмір, колір та конфігурація екранних шрифтів повинні забезпечувати комфортну роботу користувачів;
* налаштованість графічних елементів інтерфейсу, у тому числі колірного оформлення, у межах можливостей операційної системи.

У частині діалогу з користувачем графічний інтерфейс повинен відповідати наступним вимогам:

* діалог із користувачем повинен бути оптимізований для виконання типових і часто використовуваних прикладних операцій;
* при виникненні помилок у роботі підсистеми на екран монітора повинне виводитися повідомлення з найменуванням помилки й із рекомендаціями з її усунення;
* на екрані повинне здійснюватися відображення тільки тих можливостей, які доступні конкретному користувачеві й тільки необхідної для рішення поточної прикладного завдання інформації;
* повинна бути передбачена максимальна уніфікація процедур реалізації аналогічних функцій у різних підсистемах;
* повинна бути передбачена орієнтація на використання клавіатури з мінімізацією кількості натискань для стандартних дій;
* повинне бути передбачене використання функціональних і "гарячих" клавіш, при цьому на екрані повинна перебувати підказка про призначення таких клавіш;
* повинне бути передбачене використання маніпулятора "миша" на додаток до клавіатури й мінімізація кількості натискань кнопок для стандартних дій;
* повинна бути забезпечена можливість зміни складу меню користувача за допомогою настроювання параметрів підсистем;
* повинне виконуватися відображення на екрані ходу тривалих процесів обробки;
* повинна бути передбачена розвинена система контекстної допомоги.

У частині процедур вводу-виводу даних графічний інтерфейс користувача повинен відповідати наступним вимогам:

* користувач повинен мати можливість гнучко контролювати введення даних– мати можливість переглядати введені дані на моніторі, робити їх корегування, або відмовитися від введення;
* при введенні повинні використовуватися для контроля випадаючі списки даних, що вводяться, і їх допустимих значень, має бути забезпечена можливість введення значень за замовчуванням;
* повинно бути виключене повторне введення даних;
* повинен здійснюватися логічний контроль інформації, що вводиться. [16]

***Вимоги до експлуатації, технічної естетики***

Система повинна забезпечувати безперервний цілодобовий режим експлуатації з урахуванням часу на технічне обслуговування.

Для нормальної експлуатації Системи має бути забезпечено безперебійне живлення технічних засобів.

У приміщеннях, призначених для експлуатації Системи, повинні бути відсутніми агресивні середовища, масова концентрація пилу в повітрі має бути не більше 0,75 мг / м3, електрична складова електромагнітного поля перешкод не повинна перевищувати 0,3 Н/м в діапазоні частот від 0,15 до 300,00 МГц.

Напруга живлення мережі має бути 220 В, 50 Гц.

Нормальними кліматичними умовами експлуатації системи мають бути:

* температура навколишнього повітря +15 - +25°С;
* відносна вологість навколишнього повітря 75% при атмосфері повітря +18° С;
* атмосферний тиск 740 – 770 мм рт.ст.
* Система повинна зберігати працездатність при впливі наступних кліматичних факторів:
* температура навколишнього повітря від 10 до 45;
* відносна вологість повітря від 40 до 80% при температурі +10°С . [12]

Періодичне технічне обслуговування технічних засобів повинно проводитися відповідно до вимог технічної документації виробників, але не рідше одного разу на рік.

Періодичне технічне обслуговування і тестування технічних засобів повинні включати в себе обслуговування і тестування всіх використовуваних засобів, включаючи робочі станції, сервери, кабельні системи та мережеве обладнання, пристрої безперебійного живлення.

В процесі проведення періодичного технічного обслуговування повинні проводитися зовнішній і внутрішній огляд і чистка технічних засобів, перевірка контактних з'єднань, перевірка параметрів налаштувань працездатності технічних засобів і тестування їх взаємодії.

На підставі результатів тестування технічних засобів повинні проводитися аналіз причин виникнення виявлених дефектів і вживати заходів щодо їх ліквідації.

Відновлення працездатності технічних засобів повинно проводитися відповідно до інструкцій розробника і постачальника технічних засобів і документами по відновленню працездатності технічних засобів і завершуватися проведенням їх тестування.

Технологічні приміщення, у яких мають зберігатися відомості та спеціальні дані єдиної інтерактивної бази даних про кіберінциденти для потреб спеціальних установ, систем інформаційного обміну про кіберзагрози, підсистем виявлення та реагування на кібератаки на рівні кінцевих точок та збору телеметрії ІТС користувачів системи, інших відомостей, вимога до захисту яких встановлена законом, мають задовольняти вимогам до зберігання відповідних відомостей та даних, з урахуванням юридичного статусу суб’єктів, які є їх власниками або розпорядниками, відомостей та даних про вразливості ІТС користувачів системи, сукупностей цих відомостей та даних. [12][13]

***Вимоги до безпеки***

Технічні засоби системи повинні забезпечувати безпечну роботу персоналу без додаткового проведення інструктажів та спеціальної підготовки по техніці безпеки, при будь-яких, у тому числі помилкових, дій користувачів, не пов’язаних з розкриттям корпусу.

Всі зовнішні елементи технічних засобів Порталу, що знаходяться під напругою, повинні мати захист від випадкового натискання, а самі технічні засоби - мати захисне заглушення або захисну заземлення. [15]

Конструкція всіх елементів технічних засобів Системи повинна виключати можливість приєднання людини до частин і елементів під напругою більше 36 В при будь-яких, у тому числі помилкових, діях користувача, не пов'язаних з розкриттям корпусу.

Конструкція технічних засобів повинна забезпечувати безпеку експлуатуючого персоналу та користувача від удару електричним струмом. [13][14]

На частинах пристроїв, пов'язаних із діями, що представляють небезпеку, повинні бути нанесені добре помітні попереджувальні надписи ("під напругою", "не розкривати" і т.п.).

Технічні засоби повинні мати індикацію включення мережевої напруги живлення.

Допустимі рівні освітленості, звукового тиску, іонізації повітря, вібрації, а також допустимі параметри електромагнітних неіонізуючих випромінювань і електростатичного поля у приміщеннях для роботи персоналу повинні відповідати ДСанПІН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»

***Вимоги до захисту від впливу зовнішніх факторів***

Система повинна відповідати наступним вимогам щодо стійкості стабільності й витривалостідо зовнішніх впливів:

* мати можливість функціонування при коливаннях напруги електроживлення в межах від 155 до 265 В (220 ± 20% - 30%);[14]
* мати можливість функціонування в діапазоні допустимих температур навколишнього середовища, встановлених виробником апаратних засобів.
* мати можливість функціонування в діапазоні допустимих значень вологості навколишнього середовища, встановлених виробником апаратних засобів.
* мати можливість функціонування в діапазоні допустимих значень вібрацій, встановлених виробником апаратних засобів.
* електромагнітне випромінювання радіодіапазону, що виникає при роботі електропобутових приладів, електричних машин і установок, приймально-передавальних пристроїв, що експлуатуються на місці розміщення технічного обладнання Системи, не повинні призводити до порушень працездатності підсистем.[13][15]

## 2.1.5 Вимоги до захисту інформації від несанкціонованого доступу

Компоненти Системи для  роботи з інформацією з обмеженим доступом повинні відповідати вимогам до збереження інформації, викладеним у Законах України "Про захист інформації в автоматизованих інформаційних системах" (05.07.1994 N 81/94-ВР), "Про захист інформації в інформаційно-комунікаційних мережах" (05.07.1994 N 80/94-ВР), іншими нормативно-правовими актами, виданими у відповідності з цими законами, а також “Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави”, затвердженою постановою Кабінету Міністрів України від 27.11.1998 р., N 1893 (зі змінами від 07.09.2011 р.).[10][11]

Забезпечення інформаційної безпеки програмних компонентів Системи для роботи з інформацією з обмеженим доступом повинне задовольняти наступним вимогам:

* + захист повинен забезпечуватися на всіх технологічних етапах обробки інформації й у всіх режимах функціонування, у тому числі при проведенні регламентних робіт;
  + програмно-технічні засоби захисту не повинні суттєво погіршувати основні функціональні характеристики програмних компонентів Системи (надійність, швидкодію, можливість зміни конфігурації);
* У частині захисту інформації компоненти Системи для роботи з інформацією з обмеженим доступом повинні забезпечувати: [17]
* попередження порушення конфіденційності, цілісності та доступності інформації з обмеженим доступом та захисту інформаційних і програмних ресурсів;
* розмежування доступу користувачів і адміністраторів до інформації яка потребує захисту від несанкціонованого внесення змін або знищення баз даних;
* запобігання несанкціонованого використання інформації баз даних;
* контроль цілісності файлів, каталогів, елементів системного реєстру, секторів дисків;
* керування підключеннями Irda, Wifi, Firewire, Ethernet, Bluetooth;
* реєстрацію подій безпеки.[18][19]

У процесі впровадження  компоненти Системи для роботи з інформацією з обмеженим доступом повинні бути сертифіковані на відповідність комплексу засобів захисту інформаційної системи від несанкціонованого доступу вимогам нормативних документів із технічного захисту інформації.

***Вимоги до збереження інформації при аваріях***

Система повинна забезпечувати збереження даних в наступних ситуаціях:

* аварійне відключення електроживлення;
* збій або вихід з ладу технічних засобів, на яких здійснюється експлуатація системи;
* збій загального (системного) програмного забезпечення (ОС, СУБД);
* збій або відмова спеціального і прикладного програмного забезпечення;
* збій через помилкові дій персоналу.[16]

Для запобігання втрати або пошкодження інформації  в Системі повинні забезпечуватися наступні способи захисту:

* дублювання і резервування джерел і мереж електроживлення;
* дублювання і резервування даних, включаючи гаряче резервування;
* використання механізмів відкату транзакцій;
* використання схем контролю та відновлення цілісності даних;
* дублювання і резервування носіїв, накопичувачів даних, пристроїв зберігання даних і інтерфейсів до них;
* уніфікація методів і засобів зберігання даних;
* використання незалежної пам'яті для зберігання даних;
* резервне копіювання даних з віддаленим зберіганням резервних копій і застосуванням схем ротації резервних копій і носіїв;
* впровадження та налагодження документованого процесу резервного копіювання та відновлення даних, включаючи процедуру прийняття рішення на відновлення резервних копій;
* захист цілісності, доступності та конфіденційності резервних копій даних;
* забезпечення необхідної діагностики збоїв і відмов обладнання програмно-технічними засобами;
* забезпечення протоколювання подій при функціонуванні ПЗ.

При аваріях розроблюване спеціальне і прикладне програмне забезпечення Системи повинно відновлювати своє функціонування при коректному перезапуску апаратних засобів.

Для запобігання пошкодження і втрати інформації унаслідок помилок персоналу система повинна передбачати можливість розмежування прав доступу до інформації користувачів. Для різних користувачів повинні бути встановлений різні права на читання, редагування і видалення інформації в базі даних. [18]

# **2.2 Архітектура Системи (логічна компонента)**

В основі архітектури програмного забезпечення організації комплексного рішення для забезпечення збору, накопичення та попередження кіберінцидентів лежить веб-орієнтована модель додатку. Дані повинні оброблятись на сервері, а доступ користувачів до модулів Системи повинен здійснюватись за допомогою web-інтерфейсу.

До складу Системи, як центрального сегменту СКЗ, що розробляється будуть включені наступні технологічні компоненти:

* кластер закритого сегменту;
* кластер відкритого сегменту;
* мережевий екран.

Система будується на відмовостійких кластерах. Кластер закритого сегменту забезпечує роботу віртуальних машин з сервісами, які забезпечують збір, обробку та передачу користувачам Системи інформації щодо кіберзагроз та віртуальних серверів сховища даних. Кластер відкритого сегменту забезпечує роботу віртуальних машин з сервісами прийому СД з різних джерел активного та пасивного моніторингу. Кластер закритого сегменту реалізується засобами, які розробляються Виконавцем та засобами MongoDB, Redis Cache, ElasticSearch, RabbitMQ. Кластер відкритого сегменту реалізується засобами, які розробляються Виконавцем.

Для забезпечення захисту даних віртуального простору закритого сегменту Системи два кластери мають бути під’єднуватися один до одного через мережевий екран. Мережевий екран обирається та визначається Замовником на стадії підписання Договору, як додатковий компонент.

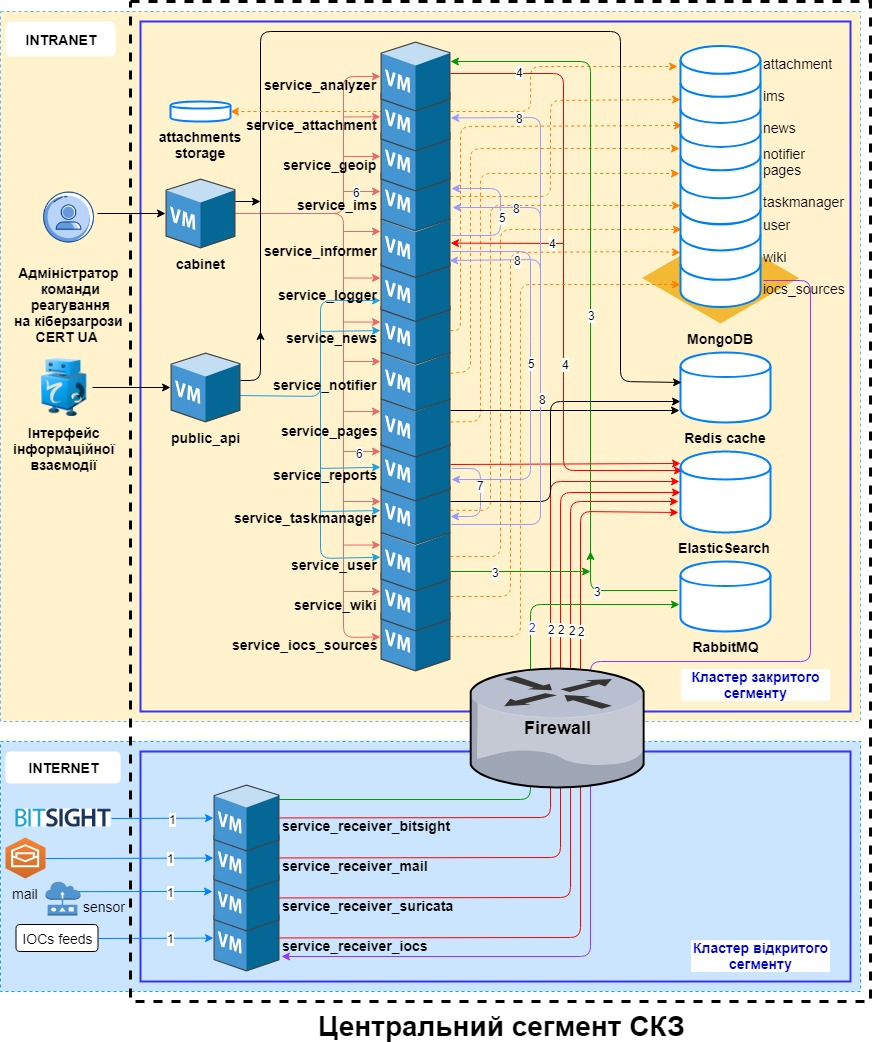


Рис. 1. Логічна і компонентна архітектура Системи

Згідно з Технічним вимогами Система включає наступні сервіси:

* особистий кабінет;
* API інтеграція з зовнішніми системами;
* сервіс прийому СД з джерела Bitsight для збору та подальшого аналізу;
* сервіс отримання індикаторів компрометації через e-mail;
* сервіс отримання даних активного моніторингу з сенсорів активного моніторингу;
* сервіс отримання індикаторів компрометації з джерел TI;
* сервіс обробки даних про кібер загрози із зовнішніх джерел;
* сервіс сховища даних;
* сервіс визначення геоположення за IP адресою;
* сервіс внутрішньої пошти;
* сервіс інформування про події системи;
* сервіс логування дій в системі;
* сервіс новин;
* сервіс сповіщення про події системи;
* сервіс статичних сторінок онлайн-кабінету;
* сервіс звітів;
* сервіс керування задачами;
* сервіс управління особистим кабінетом користувача;
* сервіс зберігання бази знань;

Призначення кожного сервісу наведені нижче в таблиці 2

Таблиця 2

|  |  |  |
| --- | --- | --- |
| № | Назва сервісу | Основне призначення сервісу |
| 1 | Особистий кабінет | Забезпечує доступ користувачам до інформації про вразливості або підозрілу активність в їх мережах, обробки даних та реагування на інциденти (блокування мережевих загроз і тп.) в залежності від прав користувачів. |
| 2 | API інтеграція з зовнішніми системами | Забезпечує інтеграцію з зовнішніми  структурними елементами для запровадження доступу до даних  Системи через інтерфейс зовнішньої взаємодії. |
| 3 | Сервіс агрегації СД з джерела Bitsight | Забезпечує прийом СД з Bitsight, зчитує, вилучає та обробляє дані, після чого представляє вилучені дані в зручному для обробки в Системі форматі. |
| 4 | Сервіс отримання індикаторів компрометації через e-mail | Забезпечує прийом та парсинг СД з різних джерел TI у вигляді електронних листів. |
| 5 | Сервіс отримання даних активного моніторингу з сенсорів активного моніторингу | Забезпечує прийом та парсинг СД активного моніторингу з сенсорів активного моніторингу. |
| 6 | Сервіс отримання індикаторів компрометації з джерел TI | Забезпечує прийом та парсинг СД пасивного моніторингу з джерел пасивного моніторингу. |
| 7 | Сервіс обробки даних про кібер загрози із зовнішніх джерел | Забезпечує збір даних з різних типів  каналів пасивного та активного моніторингу, нормалізує їх для приведення в єдиний вид та корелює за визначеними в Системі  правилами кореляції для використання Системою для подальшої роботи та зберігання. |
| 8 | Сервіс сховища даних | Забезпечує зберігання файлів різних форматів, які можуть бути прикріпленими до звітів/задач/електронних листів тощо. |
| 9 | Сервіс визначення геоположення за IP адресою | Забезпечує можливість приведення IP адрес з СД до одного формату та сортування їх по типам: регіон, район, місто, країна. |
| 10 | Сервіс внутрішньої пошти | Забезпечує створення “внутрішніх” поштових скриньок в Системі зареєстрованими користувачами та роботу з ними - прийом/відправки повідомлень. |
| 11 | Сервіс інформування про події системи | Забезпечує збирання, опрацювання та інформування про внутрішні події Системи. |
| 12 | Сервіс логування дій в системі | Забезпечує можливість повного логування дій користувачів Системи та їх фільтрації. |
| 13 | Сервіс новин | Забезпечує можливість створення та зберігання новин і заміток у Системі. |
| 14 | Сервіс сповіщення про події системи | Забезпечує збирання, опрацювання та інформування про зовнішні події Системи. |
| 15 | Сервіс статичних сторінок онлайн-кабінету | Забезпечує можливість створення сторінок з обраним контентом користувачем з відповідними правами доступу (приклад адміністратор команди CERT-UA) для перегляду всім користувачам Системи. |
| 16 | Сервіс звітів | Забезпечує можливість створення запитів, їх обробки та аналізу адміністратор команди CERT-UA (наприклад, для обробки даних із зовнішніх джерел з повідомленнями про інциденти). |
| 17 | Сервіс керування задачами | Забезпечує можливість створення задач/проектів |
| 18 | Сервіс управління особистим кабінетом користувача | Забезпечує можливість максимально зручного та простого управління особистим профілем зареєстрованого в Системі користувача. |
| 19 | Сервіс зберігання бази знань | Забезпечує можливість зберігання та структурування бази знань, виведення їх у гіпертекстовому форматі, забезпечення навігації та пошуку. |

***Засоби розробки***

При розробці Системи використовуються наступні програмні засоби:

* операційна система Ubuntu 18.04 LTS (або аналог);
* середовище розробки для PHP JetBrains PHPStorm (або аналог);
* веб-переглядач Chrome (або аналог);
* графічний редактор Adobe Photoshop (або аналог);

При розробці Системи використовувались наступні технології та мови програмування:

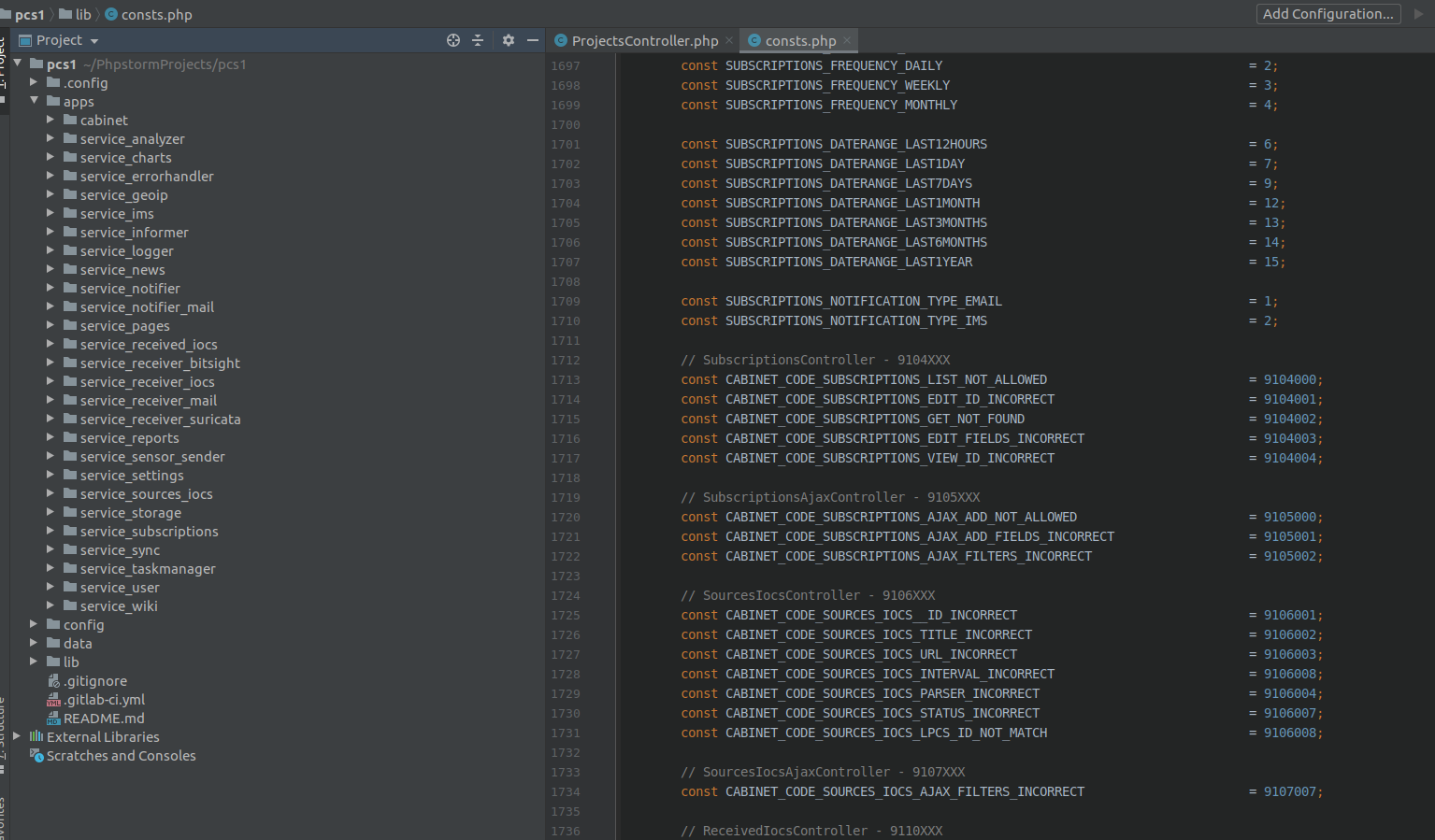
* мова програмування PHP 7 з використанням фреймворку Phalcon;
* мова програмування Node.js з використанням фреймворку express;
* мова програмування JavaScript;
* мова розмітки HTML;
* мова розмітки CSS з використанням фреймворку Bootstrap;
* MongoDB — документо-орієнтована система керування базами даних (СКБД);
* пошукова система ElasticSearch;
* Redis - розподілене NoSQL сховище пар ключ-значення, які зберігаються в оперативній пам'яті, з можливістю забезпечувати довговічність зберігання;
* RabbitMQ — платформа, що реалізує систему обміну повідомленнями між компонентами програмної системи на основі стандарту AMQP. [2]

Рис. – Приклад вигляду архітектури системи у середовищі розробки PHP JetBrains PHPStorm

# **2.3 Інтерфейс та опис функцій розділів Систем (зовнішня компонента)**

**Онлайн-кабінет**

Після розробки логічної структури основних компонентів Системи, я виконала розробку кожного розділів, що були заплановалі для реалізації. Далі я описала основні функції та задачі, що можна вирішити в кожному з модулів, а також представила фрагменти інтерфейсу програмної компоненти у вибіркових розділах.

Доступ до Системи мають лише верифіковані користувачі. Тому для того, щоб потрапити до Онлайн-кабінету, необхідно виконати авторизацію.

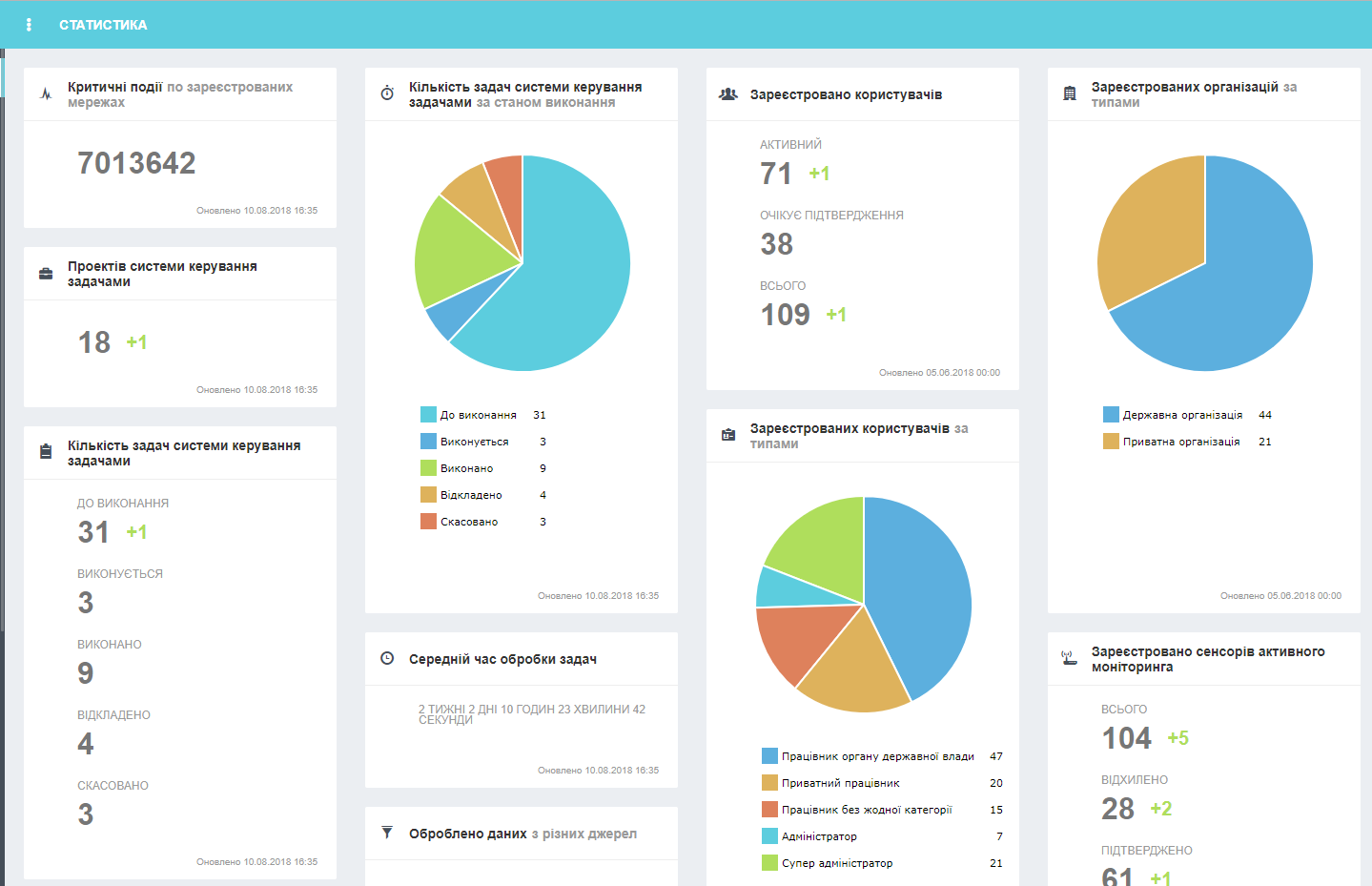
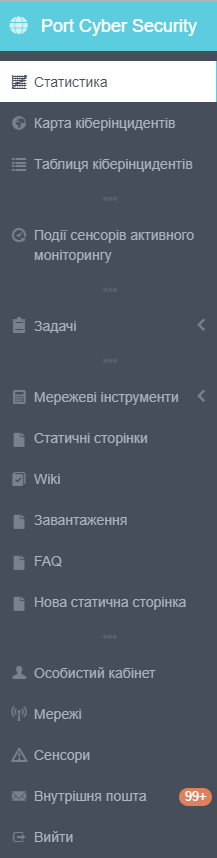


Рис. – Інтерфейс системи, модулю зі статистикою

Онлайн-кабінет містить наступні функціональні розділи:

* управління користувачами, у тому числі управління організаціями;
* налаштування мереж;
* верифікація мереж;
* управління сенсорами активного моніторингу;
* відстеження запитів клієнтів;
* звітність та статистика;
* інформування користувачів:
* мережеві інструменти;
* новини;
* часті запитання (FAQ);
* завантаження;
* обробка та візуалізація даних;
* Wiki.

Рис. – Приклад бокового меню для оналайн-кабінету

**Розділ управління користувачами**

Для того, щоб задовольнити вимоги до Системи та, водночас, поліпшити взаємозв’язок між користувачем та системиою, я вирішила відокремити чотири типи користувачів:

* користувач приватного сектору;
* користувач підключеної локальної мережі (підключеної організації);
* адміністратор;
* адміністратор найвищого рівня.

***Для користувача приватного сектору*** необхідно забезпечити виконання наступних функцій:

користувача приватного сектору

налаштування власного профілю користувача;

налаштування власної мережі), відмічання власної мережі на карті;

створення запиту клієнта та подальша робота зі своїми запитами (без можливості пріоритезації запитів);

отримання звітності та статистики у межах власної мережі;

доступ до внутрішньої системи повідомлень;

доступ до зовнішнього інформування (опціонально);

доступ до розділу мережеві інструменти (з обмеженнями);

доступ розділу новини (з обмеженнями);

доступ до розділу часті запитання;

доступ до розділу завантаження (з обмеженнями).

***Для користувача підключеної локальної мережі*** необхідно забезпечити виконання наступних функцій:

користувача підключеної локальної мережі

налаштування власного профілю користувача;

налаштування власної мережі , відмічання власної мережі на карті;

створення запиту на встановлення активного сенсору;

створення запиту клієнта та подальша робота зі своїми запитами

перегляд загальних даних профілю інших користувачів, що відносяться до даної організації;

отримання звітності та статистики у межах власної мережі;

доступ до внутрішньої системи повідомлень;

доступ зовнішнього інформування (без обмежень);

доступ розділу мережеві інструменти (без обмежень);

доступ розділу новини (без обмежень);

доступ розділу часті запитання;

доступ розділу завантаження (без обмежень);

перегляд карти зі своїми мережами;

***Для адміністратора*** необхідно забезпечити виконання наступних функцій;

для адміністратора

керування користувачами приватного сектору та користувачами підключених організацій;

верифікація користувачів підключеної організації;

можливість ручної верифікації мереж користувачів;

доступ до внутрішньої системи повідомлень;

доступ зовнішнього інформування (без обмежень);

доступ до розділу мережеві інструменти (без обмежень);

доступ розділу новини (без обмежень);

доступ до звітів та статистики для усіх мереж користувачів;

створення запиту;

опрацювання запитів клієнтів системи;

перегляд статистики відповідей на запити клієнтів;

перегляд карти усіх мереж;

перегляд дій користувачів системи (користувачів підключених організацій та користувачів приватного сектору);

***Для адміністратора найвищого рівня*** необхідно забезпечити виконання всіх функцій адміністратора, а також додаткових функцій:

для адміністратора найвищого рівня

всі функції адміністратора

+

керування усіма типами користувачів Системи;

керування організаціями Системи;

перегляд статистики відповідей на запити клієнтів (у повному обсязі);

перегляд усіх дій адміністраторів Системи

Розділ управління користувачами містить функціональні блоки:

* блок реєстрації користувачів;
* налаштування профілю користувача

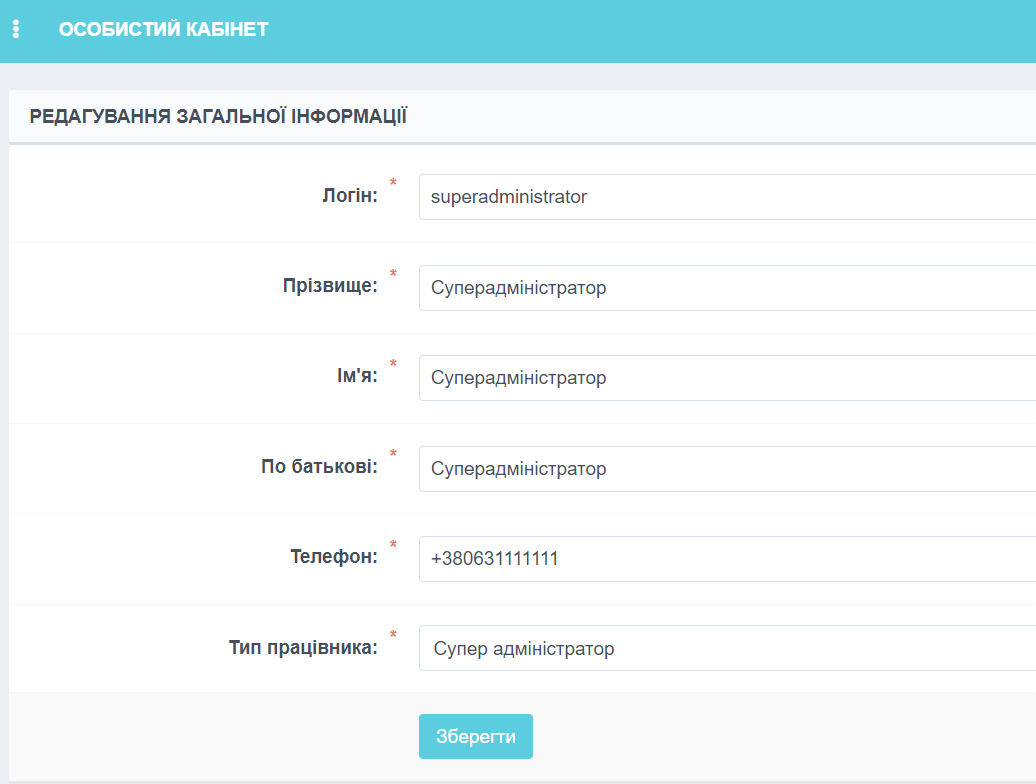


Рис. – Приклад блоку налаштування профілю користувача

Блок  реєстрації користувачів викононує основні функції:

* здійснювати логічну перевірку заповнених відомостей (наприклад, перевірка правильності формату введення телефону або електронної поштової скриньки);
* здійснювати перевірку зареєстрованої електронної поштової скриньки шляхом надсилання унікального посилання для підтвердження реєстрації скриньки;
* дозволяти реєстрацію з однаковим номером телефону тільки у тому випадку, якщо такого номеру телефону немає ні в кого з підтверджених, активних користувачів;
* мати механізм нагадування паролю із використанням вказаної адреси електронної поштової скриньки;
* забезпечувати нагадування паролю через СМС;
* забезпечувати використання двохфакторної автентифікації;
* бути стійким до кібератаки типу брутфорс;
* забезпечувати оповіщення про реєстрацію та інші дії користувачів в онлайн кабінеті адміністратора сайту через внутрішню систему повідомлень;
* забезпечувати надсилання електронних листів до користувачів системи, у тому числі:
* під час реєстрації та після її успішного завершення;
* зміни особистих даних (наприклад зміна паролю);
* зміни статусу двохфакторної автентифікації;
* забороняти реєстрацію по ІР-адресам;
* надавати доступ користувачів до розділів Системи (крім даних свого профілю) тільки після проходження верифікації зі сторони Адміністратора або Адміністратора найвищого рівня;

Розділ забезпечує можливість користувачеві відредагувати свої контактні дані, а саме:

* Логін;
* ПІБ;
* Пароль;
* Поштова адреса ;
* Увімкнення двохфакторної автентифікації.

**Розділ управління організаціями**

Система має перелік Організацій або установ, що підключені до Системи. Включення організації до переліку відбувається за письмовим поданням до організації, що здійснює керування командою CERT.

Редагування списку організацій здійснюється в ручному режимі Адміністратором найвищого рівня.

**Розділ налаштування мереж**

Розділ надає наступні можливості користувачу:

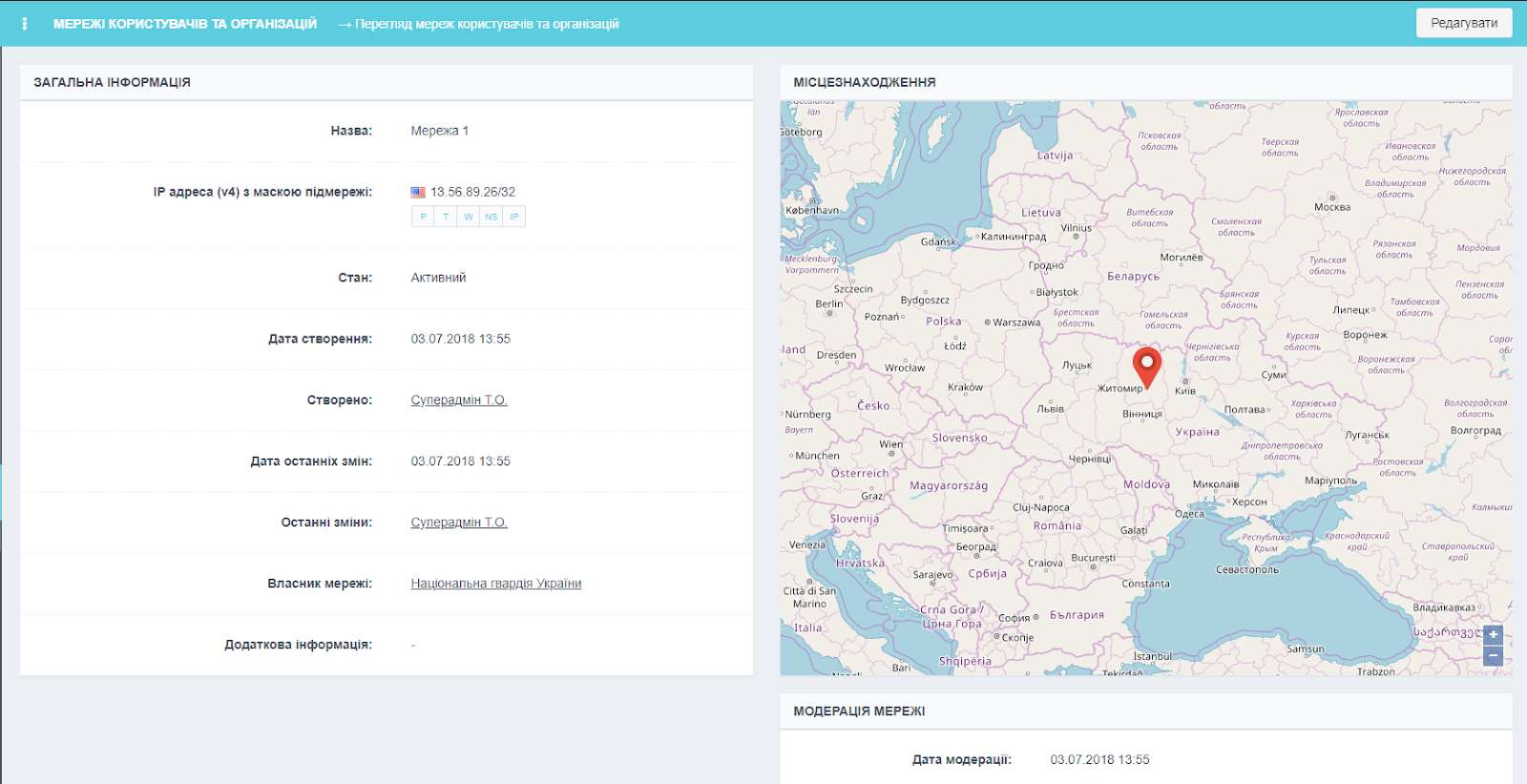
* вводити інформацію (ІР-адреси) про свою мережу та відмічати її місцезнаходження на карті для подальшої візуалізації. За вказаною інформацією користувач у майбутньому отримуватиме звіти;
* вводити назви для кожної своєї мережі;
* додатково для відстеження додавати домен сайту (також із проходженням верифікації на право управління ресурсом);
* видалення свої мережі;
* мати більше однієї мережі (після додавання, кожна окрема мережа повинна проходити окрему верифікацію на право управління ресурсом). 

Рис. – Приклад вигляду мережі

**Розділ управління сенсорами активного моніторингу**

Розділ надає можливість продивлятися спрацювання свого сенсору (декількох сенсорів) у реальному часі.

Адміністратор підключеної локальної мережі має можливість продивлятися деталі роботи сенсору тільки в межах своїх мереж, а саме:

* Статус роботи сенсора;
* Карту з розміщенням і статусами сенсорів;
* Графічне подання мережевого трафіку власних мереж;
* Детальна інформація про склад мережевого трафіку за вказаний період;
* Перегляд виявлених джерел компрометації, їхніх типів та ін.

**Розділ звітності та статистики**

Розділ дозволяє отримувати та завантажувати звіти, які формуються модулями пасивного та активного моніторингу.

Доступні дії користувача для розробленого розділу:

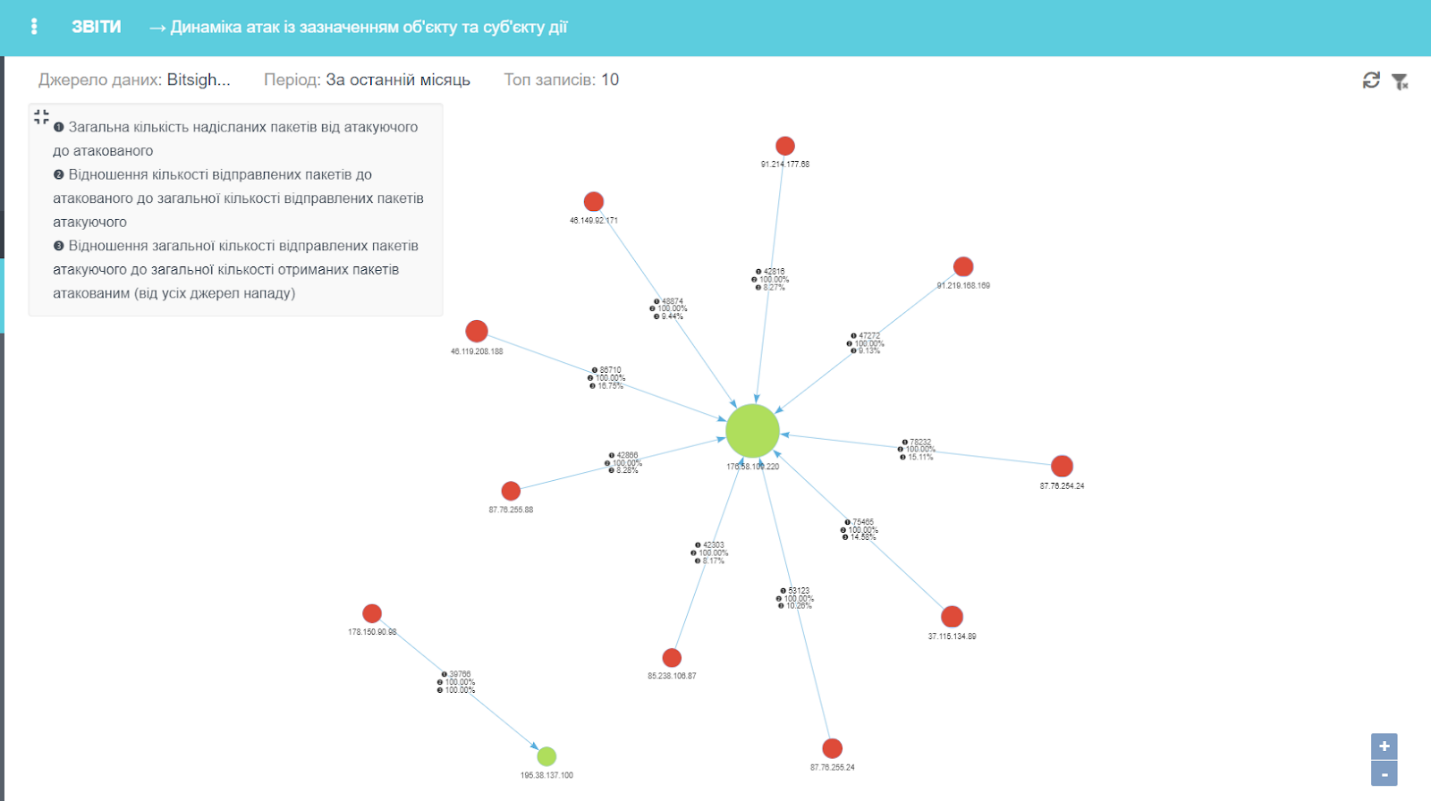
* отримувати обрані дані в онлайн-кабінеті;
* вказувати період для формування звіту, тип загроз та інші критерії, що наявні у модулях активного та пасивного моніторингу;
* завантажувати дані з можливістю вибору по фільтрам в форматах .txt, .pdf, .doc;
* отримувати на поштову адресу і/або внутрішню поштову систему обрані дані із обраною періодичністю. 

Рис. – Приклад звіту із зовнішнім джерелом даних Bitsight

**Розділ інформування користувачів**

Розділ інформування користувачів має два модуля:

* Внутрішня система повідомлень;
* Зовнішнє інформування.

Внутрішній модуль повідомлень я розробила так, щоб він сигналізував у наступних випадках:

* Зміни статусу, пріоритету запиту, створеного користувачем;
* Зміни статусу верифікації користувача, його мереж, запуску чи припинення функціонування сенсорів, що встановлені в його установі;
* Появи інцидентів у його мережі (та реакції сенсору на інцидент у разі, якщо є налаштовані політики автоматичної реакції сенсорів на інцидент);
* Внутрішньої взаємодії між користувачами системи в рамках своєї організації.

Зовнішнього модуля інформування виконує аналогічні завдання до модуля внутрішніх повідомлень, з використанням e-mail.

**Модуль збору та нормалізації даних**

Загальній функціонал модулю збору та нормалізації даних:

* збір даних з різних типів каналів пасивного та активного моніторингу (наприклад, потоки даних у реальному часі);
* нормалізація даних для приведення в єдиний вид, що використовується системою у роботі та для подальшого збереження;
* можливість додавання даних про загрози та інциденти вручну Адміністратором;
* можливість створення власного потоку нормалізованих даних для передавання у зовнішні структурні елементи.

Модуль пасивного моніторингу забезпечує:

* обробку інформації, яка надходить до центру кібербезпеки з різних джерел у вигляді електронних листів, звітів, мережевого потоку, звернень;
* обробку отриманої інформації, формування звітів.

Перелік джерел з яких надходить інформація:

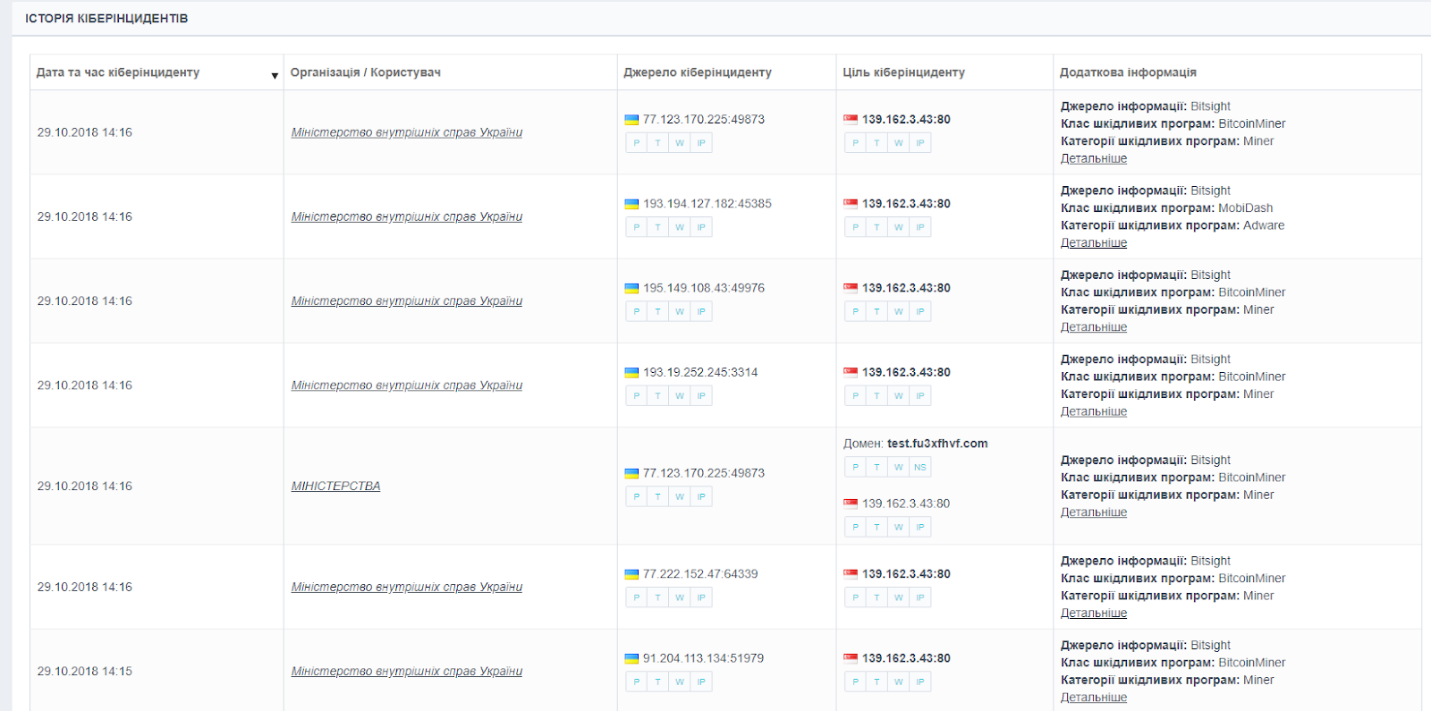
* Bitsight;
* дані, внесені Адміністратором Системи, про загрози та інциденти через окремий модуль;

Рис. – Приклад списку кіберінцидентів

Розгортання модуля пасивного моніторингу я здійснила на віртуальному сервері з ОС Ubuntu.

Модуль активного моніторингу забезпечує:

* розробку/модернізацію програмного засобу для моніторингу/блокування мережевих загроз (IDS/IPS);
* експорт даних з сенсорів до сервера баз даних;
* роботу розділу з візуалізацією виявлених загроз в онлайн-кабінеті;
* розподілення прав доступу користувачам до даних сенсорів тільки у межах своїх Організацій.

**Модуль накопичення даних моніторингу**

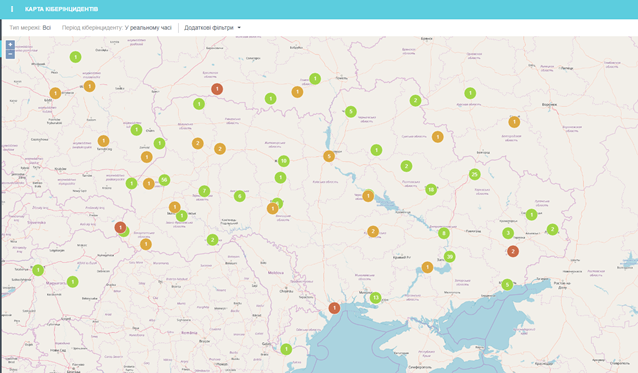
Усі наявні дані про кіберзагрози та інциденти, джерела компрометації та інша інформація, що надходить з джерел активного та пасивного моніторингу повинні зберігатися у Системі не менше трьох років.

Дані моніторингу повинні бути зарезервовані із використанням зовнішніх ресурсів.

**Модуль обробки та візуалізації даних**

Модуль візуалізації аналітичних даних виконан як веб-додаток, представлений у вигляді динамічно обновлюваної карти України.

1. Карта України, на якій відображено локації підключених організацій із зазначенням їх ІР-адреси.

Якщо ІР-адреси підключеної організації немає в БД скомпрометованих, то маркер має бути зеленого кольору. Якщо в БД є скомпрометована ІР-адреса, яка належить підключеній організації, маркер державного органу має змінювати колір на червоний. При натисканні на маркер показується інформація щодо вразливостей на конкретних ІР-адресах. 

2. Карта усіх скомпрометованих ІР-адрес України.

Карта України, на якій мають відображатися усі скомпрометовані за останні півроку ІР-адреси, які знаходяться в БД.

ІР-адреси помічаються маркерами червоного кольору, якщо вони заражені шкідливим ПЗ, жовтого кольору – якщо є інші вразливості. При натисканні на маркер виводити перелік типів вразливостей обраної ІР-адреси. Для реалізації використовується БД скомпрометованих ІР-адрес, БД геолокацій ІР та БД підключених організацій.

# **2.4 Функціональна структура Системи (внутрішня компонента)**

Система реалізовує модульний принцип побудови. Організація модулів мусить здійснюватися довкола функцій, визначених в Технічному завданні.

Модулі Системи представлені мікросервісами на віртуальних машинах. Кожний мікросервіс був розгорнутий на окрему віртуальну машину/контейнер. Мікросервіси в свою чергу об'єднувались за функціоналом в підсистеми. На Рис. 2 зображена функціональна схема Системи взаємодії підсистем обох кластерів.

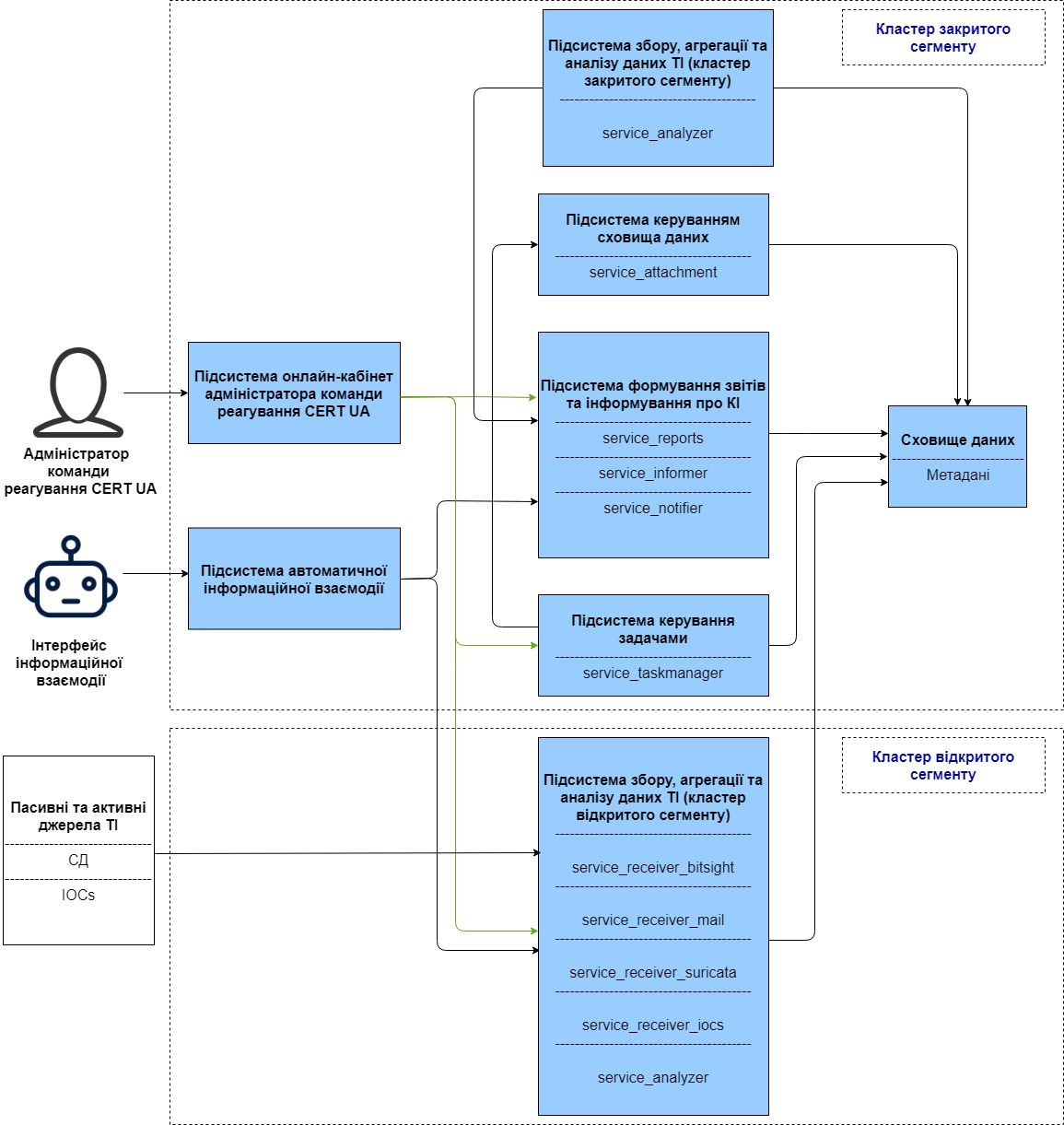


Рис. 2. Функціональна схема Системи

**Підсистема онлайн-кабінет адміністратора команди реагування**

Онлайн-кабінет представляє собою веб-портал, який дає можливість доступу користувачам до модулів Системи за допомогою web-інтерфейсу після авторизації зареєстрованої особи. Онлайн-кабінет має надавати доступ про вразливості або підозрілу активність в мережах.

Дана підсистема містить наступні функціональні розділи:

* управління користувачами, у тому числі організаціями;
* налаштування мереж;
* верифікація мереж;
* управління сенсорами активного моніторингу;
* відстеження запитів клієнтів;
* звітність та статистика;
* інформування користувачів;
* мережеві інструменти;
* новини;
* часті запитання (FAQ);
* завантаження;
* обробка та візуалізація даних;
* Wiki.

**Підсистема автоматичної інформаційної взаємодії**

Підсистема АРІ повинна реалізовувати можливість інтеграції з зовнішніми структурними елементами для запровадження доступу до даних Системи:

* Звітність та статистика;
* Інформування про наявні кіберзагрози та кіберінциденти;
* Рекомендації щодо попередження кіберінцидентів;
* Інформація про стан запитів користувача.

Можливість доступу до API повинен здійснюватися лише з використанням особистого ключа, який створюється для кожного користувача окремо і може бути отримано в онлайн-кабінеті.

**Підсистема збору, агрегації та аналізу даних з джерел ТІ (кластер закритого сегменту)**

Загалом розроблювана Система має змогу забезпечувати обробку великої кількості СД активного та пасивного моніторингу, мінімум котрих має сягає семидесяти тисяч подій в секунду. Підсистема збору, агрегації та аналізу даних з джерел ТІ, яка входить до кластеру закритого сегменту, повинна забезпечити кореляцію надходжуваного потоку СД за правилами, які будуть встановлені користувачами Системи.

Дана підсистема має налаштований зв'язок зі сховищами даних, підсистемою онлайн-кабінету та підсистемою формування звітів та інформування про КІ.

Підсистема забезпечує:

* Збір даних з різних типів каналів пасивного та активного моніторингу (наприклад, потоки даних у реальному часі);
* Кореляцію даних для формування списків загроз та спрямованих потоків навантаження Системи;
* Можливість додавання даних про загрози та інциденти вручну Адміністратором команди реагування.

**Підсистема керування сховища даних**

Підсистема керування сховища даних передбачає зберігання всіх вкладених файлів онлайн. Під вкладеними файлами маються на увазі файли, які можна відкрити через посилання та файли, які зберігаються із PDF-файлами.

**Підсистема формування звітів та інформування про КІ**

Підсистема формування звітів та інформування про КІ інформує адміністратора Системи через внутрішню пошту про надходження сповіщень про виявлення компрометованої активності з підсистеми збору, агрегації та аналізу даних з джерел ТІ кластеру закритого сегменту. Підсистема повинна надати список КІ у вигляді таблиці для перегляду власних мереж для адміністратора, після чого буде можливо створення звіту для подальших дій.

Дана підсистема має налаштований зв'язок зі сховищами даних, підсистемою онлайн-кабінету та підсистемою керування задачами/проектами та користувачами.

**Підсистема керування задачами та користувачами**

Підсистема керування задачами та користувачами охоплює собою функціонал адміністрування задачами, які мають створюватися  у відповідь на сповіщення, отримані від підсистеми формування звітів та інформування про КІ. Також до функцій підсистеми входять:

* створення задач/проектів;
* призначення пріоритету виконання задачі/проекту;
* обрання та призначення виконавця чи виконавців.

Після оформлення задачі та призначення виконавця підсистема відправляє повідомлення на внутрішню електронну пошту користувача Системи, на якого буде делегована задача та повідомляє підсистему формування звітів про створення нової задачі та додавання її до загального списку.

**Підсистема збору, агрегації та аналізу даних з джерел ТІ (кластер відкритого сегменту)**

Підсистема збору, агрегації та аналізу даних з джерел ТІ, яка входить до кластеру відкритого сегменту, забезпечує прийом та парсинг СД, які надходять з джерел активного та пасивного моніторингу в Систему.

Підсистема забезпечує:

* Прийом та обробку індикаторів компрометації, які надходить до Системи з різних джерел ТІ у вигляді електронних листів, звітів, мережевого потоку, звернень тощо;
* Обробку отриманої інформації, формування звітів зі сповіщеннями, які будуть передані до бази даних кластера відкритого сегменту для подальшої обробки;
* Експорт СД з сенсорів, які представляють собою джерела активного моніторингу в Системі.

**Сховище даних**

Дані, які надходять до Системи з різних джерел інтегровані у єдине сховище даних для можливості аналізу інформації та генерування звітів.

Для спільного використання даних здійснюється інтеграція різних СОД на основі єдиного довідника метаданих, тобто по кожному новому запиті передбачається динамічне вивантаження даних з різних СОД, їхнє узгодження, агрегація і транспортування користувачу. Дані в різних СОД можуть бути не погоджені між собою, інформація в них може бути по-різному структурована.

Сховище даних забезпечує збереження даних в хронологічному порядку, з метою можливості рішення задач прогнозування й аналізу тенденцій, та вчасного попередження користувачів Системи про мережеву небезпеку.

# **Висновки до розділу**

У даному розділі було розглянуто процес розробки системи та її складових, логічну структуру та архітектуру програмної системи.

Для початку, були сформовані вимоги до її роботи, а саме вимоги до функціонування системи, вимоги до надійності, вимоги до взаємодії із зовнішніми системами та інші.

Було розроблено архітектуру системи, виділені основні сервіси та технологічні компоненти, а також їх характеристики та функції.

Засобами розробки було обрано середовище розробки для PHP JetBrains PHPStorm, мова програмування PHP 7 з використанням фреймворку Phalcon та JavaScript, а також мова розмітки HTML та CSS з використанням фреймворку Bootstrap, пошукова система ElasticSearch та MongoDB — документо-орієнтована система керування базами даних (СКБД).

Після цього було реалізовано програмну частину та описані результати, а також її зовнішній вигляд.

# **РОЗДІЛ 3 – ДОСЛІДЖЕННЯ ПРОГРАМНОЇ КОМПОНЕНТИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ**

# **3.1 Випробування системи**

**Перелік етапів випробувань та перевірок**

Після створення Системи, я провела декілька етапів випробувань системи для оцінки відповідності між створеними вимогами та іх виконанням.

В процесі проведення випробувань були протестовані наступні підсистеми Системи:

* підсистема онлайн-кабінет адміністратора команди реагування
* підсистема автоматичної інформаційної взаємодії;
* підсистема збору, агрегації та аналізу даних з джерел ТІ (кластер закритого сегменту);
* підсистема керування сховища даних;
* підсистема формування звітів та інформування про КІ;
* підсистема керування задачами та користувачами;
* підсистема збору, агрегації та аналізу даних з джерел ТІ (кластер відкритого сегменту);
* сховище даних.

Я провела випробування всіх підсистем одночасно для перевірки їх на коректність взаємодії між собою, вплив підсистем одна на одну, тобто комплексно.

Також додатково я включила перевірку:

* повноти і якості реалізації функцій, зазначених у ТЗ;
* виконання кожної вимоги, що відноситься до інтерфейсу Системи;
* роботи користувачів в діалоговому режимі;
* повноти дій, доступних користувачеві, і їх достатність для функціонування Системи;
* складності процедур діалогу, можливості роботи користувачів без спеціальної підготовки;
* реакції Системи на помилки користувача;
* практичної виконуваність рекомендованих процедур.

**Випробування підсистеми автоматичної інформаційної взаємодії**

Випробування підсистеми автоматичної інформаційної взаємодії направлені на перевірку загальної продуктивності всієї Системи і з'ясувати відносний час затримки при виконанні кожної фази загального процесу обробки даних. Такі випробування слугують основою для створення висновків про оптимальність використовуваної Системи.

Вимоги до взаємозв'язків та роботи сервісів, які входять до складу даної підсистеми наведені в Технічному завданні.

**Випробування підсистеми збору, агрегації та аналізу даних з джерел ТІ (кластер закритого сегменту)**

Випробування підсистеми збору, агрегації та аналізу даних з джерел ТІ кластеру закритого сегменту спрямовані на перевірку відображення карти та таблиці кіберінцидентів з Bitsight та інших джерел СД активного та пасивного моніторингу. Такі випробування необхідні для перевірки коректності забезпечити кореляції надходжуваного потоку СД за правилами, які будуть встановлені користувачами Системи.

Перевірка виконувалась через веб-інтерфейс та дані перевірки повинні відповідати завданням описаних у Настанові користувача.

**Випробування підсистеми керування сховища даних**

Випробування підсистеми керування сховищами даних проводиться для перевірки можливості вводити, обробляти і отримувати доступ до всіх вкладених файлів онлайн. А також наявності можливості відкриття та перегляду файлів через посилання.

**Випробування підсистеми формування звітів та інформування про КІ**

Випробування підсистеми формування звітів та інформування про КІ спрямовані на перевірку надсилання повідомлень про надходження сповіщень про виявлення компрометованої активності з підсистеми збору, агрегації та аналізу даних з джерел ТІ кластеру закритого сегменту через внутрішню пошту для своєчасного інформування адміністратора Системи. Перевіряються процедури і параметри:

* наявність таблиці з переліком мереж;
* побудова звітів по наявним в Системі шаблонах;
* коректна роботи внутрішньої пошти.

**Випробування підсистеми керування задачами та користувачами**

Випробування підсистеми керування задачами та користувачами були направлені на перевірку:

* створення користувача в Системі;
* перехід до розділу керування користувачами;
* надання прав користувачу та перевірка коректного відображення модулів, до яких наданий доступ;
* створення задачі/проекту;
* створення групи користувачів;
* редагування задачі/проекту;
* додавання організації;
* перегляд інформації про користувача/організацію.

**Випробування підсистеми збору, агрегації та аналізу даних з джерел ТІ (кластер відкритого сегменту)**

Випробування підсистеми збору, агрегації та аналізу даних з джерел ТІ кластеру відкритого сегменту спрямовані на забезпечення коректної інтеграції з існуючими джерелами пасивного та активного моніторингу, такими, як:

* Bitsight;
* сенсори активного моніторингу;
* джерела СД ТІ.

Інтеграція з зазначеними компонентами повинна здійснюватися за допомогою надання веб інтерфейсу для даних компонентів. Перевіряється коректність відображення інформації.

**Випробування підсистеми сховища даних**

Випробування підсистеми сховища структурованих даних і метаданих про процеси і документах спрямовані на перевірку зберігання в БД Системи і вибірки з БД об'єктів для коректної роботи PCS.

Вимоги до Сховища структурованих даних і метаданих про процеси і документи наведені в Технічному завданні.

**Методика проведення випробувань**

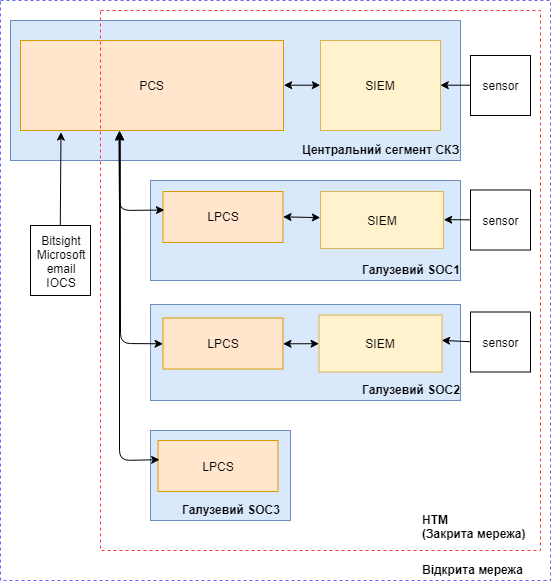
В таблиці нижче я описала типові сценарії дій, які будуть найчастіше виконуваними в Системі.

|  |  |  |
| --- | --- | --- |
| № | Дія | Результат |
| 1. | Сценарій “Авторизація” | |
|  | Вхід до Системи під користувачем з правами Адміністратора команди реагування CERT-UA. | Авторизація пройшла успішно, при відсутності діагностичних повідомлень про помилки. |
| 2. | Сценарій “Перегляд профілю” | |
|  | У випадаючому меню зліва обрати підрозділ “Особистий кабінет” та натиснути на назву. | Виконується перехід на сторінку “Особистого кабінету”, де будуть відображатися підрозділи “Редагування загальної інформації”, “Змінити пароль”, “Змінити email”, “Двоетапна перевірка”, “Доступ до публічного API”. |
| 2.1. | Зміна інформації в підрозділі “Редагування загальної інформації”, заповнення всіх рядків з зірочкою. Натиснути кнопку Зберегти. | Виконується заміна попередніх даних та зберігання останніх введених даних. |
| 2.2. | Заповнення чекбоксу “Змінити пароль”, “Змінити email”, “Двоетапна перевірка”, “Доступ до публічного API”. Натиснути кнопку Зберегти після заповнення обов'язкових рядків. | Виконується заміна попередніх даних та зберігання останніх введених даних. |
| 3. | Сценарій “Перегляд та додавання мереж” | |
| 3.1. | У випадаючому меню зліва обрати підрозділ “Мережі” та натиснути на назву. | Виконується перехід на сторінку “Мережі”, де будуть відображатися мережі доданих до Системи користувачів у вигляді таблиці. |
| 3.2. | У верхній частині сторінки обрати необхідний фільтр для пошуку за IP адресами, за станом мережі, за станом їх модерації та додатковими фільтрами (Назва, Створено, Дата створення, Оновлено, Дата останніх змін). | Відобразиться список з переліком мереж за заданими фільтрами у вигляді таблиці. |
| 3.3. | Натиснути на знак Детальніше в останній колонці. | Виконується перехід на сторінку з інформацією про обрану мережу. |
| 3.4. | У верхньому правому кутку сторінки натиснути на “плюс”. | Виконується перехід на сторінку “Додавання мережі” з формою Загальна інформація для заповнення та картою для отримання інтерактивного місцезнаходження. |
| 3.5. | Заповнити всі поля у формі Загальна інформація та натиснути на галочку. | Виконується додавання нової мережі до загального списку. |
| 4. | Сценарій “Перегляд та додавання сенсорів” | |
| 4.1. | У випадаючому меню зліва обрати підрозділ “Сенсори” та натиснути на назву. | Виконується перехід на сторінку “Сенсори”, де будуть відображатися сенсори доданих до Системи користувачів у вигляді таблиці. |
| 4.2. | У верхній частині сторінки вибрати необхідний фільтр для пошуку за назвою, станом, за станом модерації та додатковими фільтрами (Створено, Дата створення, Оновлено, Дата останніх змін). | Відобразиться список з переліком сенсорів за заданими фільтрами у вигляді таблиці. |
| 4.3. | Натиснути на знак Детальніше в останній колонці. | Виконується перехід на сторінку з інформацією про обраний сенсор. |
| 4.4. | Натиснути на знак Події сенсора активного моніторингу в останній колонці. | Виконується перехід на сторінку “Події сенсорів активного моніторингу”. |
| 4.5. | У верхньому правому кутку сторінки натиснути на “плюс”. | Виконується перехід на сторінку “Додавання особистого сенсора активного моніторингу” з формою Загальна інформація для заповнення та картою для отримання інтерактивного місцезнаходження. |
| 4.6. | Заповнити всі поля у формі Загальна інформація та натиснути на галочку. | Виконується додавання нового сенсору в Системі. |
| 5. | Сценарій “Створення задачі” (“Створення проекту”) | |
| 5.1. | У випадаючому меню зліва обрати підрозділ “Задачі” (“Проект”) та натиснути на назву Задачі з випадаючого списку. | Виконується перехід на сторінку “Задачі”, де будуть відображатися задачі створені адміністратором у відповідь на сповіщення від сенсорів у вигляді таблиці. |
| 5.2. | Додавання, редагування та видалення задач/ проектів здійснюється подібно до сценаріїв “Перегляд та додавання мереж” та “Перегляд та додавання сенсорів” | |
| 6. | Сценарій “Створення звіту” | |
| 6.1. | У випадаючому меню зліва обрати підрозділ “Звіти” та натиснути на назву. З випадаючого списку вибрати необхідний тип звіту. | Перехід на сторінку обраного типу звіту, де можна переглянути інформацію щодо загальної кількості надісланих пакетів від атакуючого до атакованного, відношення кількості відправлених пакетів до атакованного до загальної кількості відправлених пакетів атакуючого тощо. |
| 6.2. | У верхній частині сторінки вибрати необхідний фільтр для пошуку за джерелом даних, період та топ записів. | Відобразяться відфільтровані дані  у вигляді графіку та таблиці. |
| 7. | Сценарій “Перегляд кіберінцидентів із Bitsight” | |
| 7.1. | У випадаючому меню зліва обрати підрозділ “Перегляд кіберінцидентів із Bitsight” та натиснути на назву. | Виконується перехід на сторінку “Кіберінциденти із Bitsight”, де будуть відображатися зафіксовані та агреговані кіберінциденти Системи у вигляді таблиці. В таблиці визначені дата та час кіберінциденту, клас шкідливих програм, джерело події (IP порт), Ціль події (IP порт), протокол передачі та додаткова інформація. |
| 7.2. | У верхній частині сторінки вибрати необхідний фільтр для пошуку за періодом події, та додатковими фільтрами (Джерело події (IP), Джерело події (Порт), Ціль події (IP), Ціль події (Порт), Протокол, Клас шкідливих програм). | Відобразиться список з переліком кіберінцидентів із Bitsight за заданими фільтрами у вигляді таблиці. |
| 7.3. | Натиснути на знак Детальніше в останній колонці. | Виконується перехід на сторінку з загальною інформацією про обраний кіберінцидент з вказанням ID події. |
| 8. | Сценарій “Обмеження доступу по IP” | |
| 8.1. | У випадаючому меню зліва обрати підрозділ “Обмеження доступу по IP” та натиснути на назву. | Виконується перехід на сторінку “Обмеження доступу по IP”, де будуть відображатися IP адреси з маскою підмережі у вигляді таблиці. |
| 8.2. | Натиснути на знак Редагувати в останній колонці. Внести зміни та натиснути галочку у правому верхньому кутку. | Виконується перехід на сторінку з загальною інформацією про обрану IP адресу. В даному підрозділі вказані безпосередньо назва IP адреси, дата та час початку обмеження доступу та завершення обмеження доступу, стан адреси та додаткова інформація. Виконується зміна інформації в обраному рядку та здійснюється збереження даних. |
| 8.3. | У верхньому правому кутку сторінки натиснути на “плюс”. Натиснути галочку у правому верхньому кутку. | Виконується перехід на сторінку “Додавання обмеження доступу по IP” з формою Загальна інформація для заповнення. Обов'язковими для заповнення є поля з зірочками. Виконується збереження після натискання галочки. |

# **3.2 Сумісність Системи із зовнішніми системами**

Система є відкритою для суміжних (локальних) систем і може підтримувати можливість експорту даних в суміжні системи через інтерфейсні таблиці або файли даних. Також Система забезпечує можливість завантаження даних, одержуваних від суміжної системи.

Взаємодія Системи з Центральним сегментом СКЗ приведена на Рис.



В процесі функціонування Система може бути технологічно інтегрованою із зовнішніми системами (зовнішніми структурними елементами), включаючи, такими:

* Системи обробки та зберігання даних (єдиний основний та резервний захищений дата-центр збереження інформації і відомостей державних інформаційних ресурсів);
* Захищені вузли Інтернет-доступу;
* Ситуаційні центри суб’єктів забезпечення кібербезпеки.

Зовнішні структурні елементи можуть взаємодіяти і/або мати можливість тісної технологічної інтеграції з Системою та її внутрішніми структурними елементами за допомогою відкритих та спеціалізованих інтерфейсів, протоколів та методів із застосуванням технологій забезпечення конфіденційності та цілісності даних, що передаються.

Архітектура Системи передбачає інтерфейси взаємодії з ІТС підприємств і організацій будь-якої форми власності;

Кількісні показники щодо кожної з підсистем розраховані з урахуванням поточних потреб та технологічної готовності об’єктів, з якими має взаємодіяти підсистеми. Загальні кількісні показники та етапність робіт з впровадження підсистем визначені на етапі технічного проектування.

Зовнішні структурні елементи можуть взаємодіяти і/або мати можливість тісної технологічної інтеграції з НСКЗ та її внутрішніми структурними елементами за допомогою відкритих та спеціалізованих інтерфейсів, протоколів та методів із застосуванням (де це є можливим) технологій забезпечення конфіденційності та цілісності даних, що передаються,

Архітектура Системи передбачає інтерфейси взаємодії з:

• ІТС органів державної влади;

• ІТС підприємств і організацій будь-якої форми власності, що є володільцями (розпорядниками) критичної інфраструктури та критичної інформаційної інфраструктури;

• ІТС компаній і підприємств приватної форми власності.

# **Висновки до розділу**

В останньому розділі було проведено комплексну перевірку роботи системи: відбір вимог для випробувань, створення типових сценаріїв дій, які будуть найчастіше виконуваними в Системі та їх перевірка.

В кінці розділу було описано подальші можливості для взаємодії з іншими системами та можливості її інтегрування.

# **ВИСНОВОК**

Під час виконання дипломної роботи було проаналізовано основні поняття в сфері кіберзахисту інформаційних ресурсів в системі національної інформаційної безпеки, було виділено основні проблеми безпечного функціонування систем НСКЗ, а саме для електронного урядування, було прийняте рішення про методи та засоби реалізації системи. Також булі сформовані вимоги до такої системи, створено архітектуру та функціональні компоненти з їх подальшою розробкою. В завершальному етапі було проведено тестування функціональності системи та способи її інтеграції.

В першому розділі було визначено основні проблеми функціонування електронного уряду, дослідження існуючих систем для забезпечення ІБ, а також обрано спосіб рішення проблеми шляхом створення системи захисту інформаційних ресурсів, а саме програмну систему.

У другому розділі було сформовано основні вимоги (надійності, безпеки, несанкціонованого доступу та інші), було обрано архітектуру програмної компоненти, а також засоби для її реалізації. Розробка проводилась обраними засобами, а її результати представленні для кожного розділу з рисунками зовнішнього вигляду системи.

У третьому розділі було проведено випробування системи за типовими сценаріями, а також описана сумісність системи та її інтеграції із зовнішніми системами.

Виконуючи дипломну роботу, було вирішено такі задачі:

* Аналіз існуючих систем та підходів до їх реалізації
* Визначення способу для удосконалення існуючої системи
* Визначення вимог та задач, які система має реалізувати
* Формування архітектури програмної компоненти
* Розробка основних модулів та їх тестування
* Випробування готової програмної системи

# **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ**

1) АНДРУХІВ А.І., Порівняння методів оцінки захищеності корпоративних інформаційних систем // ТАРАСОВ Д.О. – 2006.

2) Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М. // - 2017. – 72 с.

3) Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю.О. Розширення термінології сучасного кіберпростору / Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю. О. [Електронний ресурс]. — Режим доступу: mino.esrae.ru/pdf/2014/3Sm/1387.doc

4) Ткачук Н.А. АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ СОВРЕМЕННОЙ СФЕРЫ БЕЗОПАСНОСТИ / [Електронний ресурс]. — Режим доступу: <https://elibrary.ru/item.asp?id=36296134>

5) Web application security essentials for PHP developers: The art of not getting hacked - [Електронний ресурс]. — Режим доступу : <https://www.butterfly.com.au/blog/website-development/web-application-security-essentials-for-php-developers-the-art-of-not-getting-hacked>

6) Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. –

К.: Університет «Україна»// - 2014. – с. 17-30

7) АНДРУХІВ А.І., ТАРАСОВ Д.О. «Порівняння методів оцінки захищеності корпоративних інформаційних систем» // - 2006. - Т. 2, № 4. – С. 40–53

8) Качанов С.А. Методическое пособие по разработке организационных документов по созданию и развитию аппаратно-программного комплекса «Безопасный город» // Безопасность. - 2016. - Вип. 46. – С. 21–37

9) Закон України «Про електронні документи та електронний документообіг».

10) Закон України "Про захист інформації в автоматизованих інформаційних системах" (05.07.1994 N 81/94-ВР)

11) Закон України "Про захист інформації в інформаційно-комунікаційних мережах" (05.07.1994 N 80/94-ВР)

12) ГОСТ 12.1.004-91 "ССБТ. Пожежна безпека. Загальні вимоги"

13) ГОСТ 12.2.003-91 «Обладнання Виробниче. Загальні вимоги безпеки»

14) ГОСТ 12.2.007-75 «Загальні вимоги безпеки»

15) ГОСТ 12.1.030-81 «Електробезпека. Захисне заземлення. Занулення»

16) НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

17) НД ТЗІ 1.1-004-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»

18) НД ТЗІ 2.5-008-2002 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»

19) НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі";

20) СеменченкоА. І. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури / Д. В. Мялковський, Т. В. Станіславський // Державне управління. – 2018 – С. 88-94

21) Ліпкан В. А. Поняття системи забезпечення національної безпеки України / В. А. Ліпкан // Право і Безпека. — 2003. — Т. 2, № 4. — С. 57-60.

22) Доктрина інформаційної безпеки України // <http://www.president.gov.ua/documents/472017-21374>

23) Діордіца І. В. Поняття та зміст національної системи кібербезпеки / І. В. Діордіца [Електронний ресурс]. — Режим доступу : <http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/>

24) Ліпкан В.А., Діордіца І. В. Національна система кібербезпеки як складової системи забезпечення національної безпеки україни / [Електронний ресурс]. — Режим доступу : <http://stratcom.co.ua/natsionalna-sistema-kiberbezpeki-yak-skladovoyi-sistemi-zabezpechennya-natsionalnoyi-bezpeki-ukrayini/>

25) УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» / [Електронний ресурс]. — Режим доступу : <https://www.president.gov.ua/documents/962016-19836>

26) Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 2: Електронне урядування: основи та стратегії реалізації / [А.І. Семенченко, А.О. Серенок]. – К.: ФОП Москаленко О.М., 2017. – 72 с.

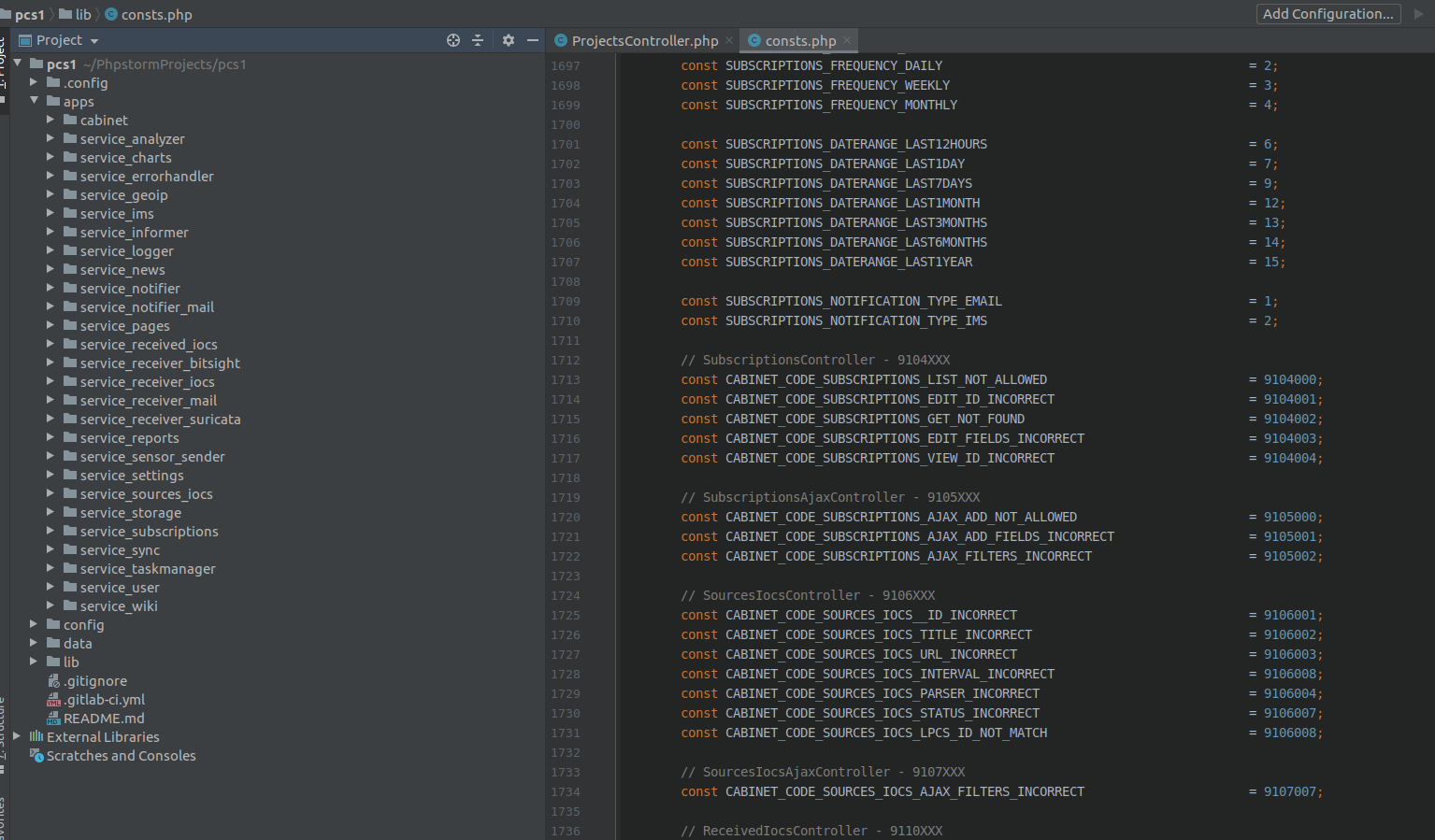
27) Інтеграція інформаційних систем / [Електронний ресурс]. — Режим доступу: <http://um.co.ua/1/1-1/1-11150.html>

28) Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – с. 50-55

29) [Електронний ресурс]. — Режим доступу: <https://zaxid.net/v_ukrayini_bude_stvorena_natsionalna_sistema_kiberbezpeki_n1380648>

30) Буйницька О. П. Інформаційні технології та технічні засоби навчання [навч. посіб.] О. П. Буйницька. — К.: Центр учбової літератури, 2012. — с. 48

**Додаток А**

**Фрагмент вихідного коду програмного засобу**