**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

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

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК 004.9

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Удосконалення модуля обліку інформаційних активів для підвищення інформаційної безпеки

|  |  |
| --- | --- |
| **Автор:** | О.Є.Бухтіяров |
| **Науковий керівник:** к.т.н., доц. | Н.К. Гулак |
| **Нормоконтролер:** асист. | С.В. Єгоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Навчально-науковий інститут інноваційних освітніх технологій**

**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 Бухтіярова Олексія Едуардовича**

1. Тема: Удосконалення модуля обліку інформаційних активів для підвищення інформаційної безпеки

затверджена наказом ректора від 22.11.2019 р. № 2701/ст.

1. Термін виконання з 25.11.2019 р. по 29.02.2020 р.
2. Вихідні дані: загрози інформаційної безпеки та їх моделі; способи реалізації загроз; система управління інформаційної безпеки; моделі порушників інформаційної безпеки; мова програмування «Java».
3. Зміст пояснювальної записки: аналіз сукупності відомостей про уразливості, загрози та атаки в інформаційних системах; дослідження методів та засобів управління комплексними системами захисту інформації; розробка програмного коду модуля інвентаризації інформаційних активів та оцінка підвищення рівня його захищеності.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Уточнення постановки задачі |  | *Виконано* |
|  | Аналіз літературних джерел |  | *Виконано* |
|  | Обґрунтування вибору рішення |  | *Виконано* |
|  | Збір інформації |  | *Виконано* |
|  | Дослідження сучасних систем і методик аналізу та оцінки ризиків інформаційної безпеки |  | *Виконано* |
|  | Формування моделі порушника й на основі аналізу обрання засобу управління та обробки ризиків |  | *Виконано* |
|  | Розробка програмного коду модуля інвентаризації інформаційних активів |  | *Виконано* |
|  | Перевірка на антиплагіат |  | *Виконано* |
|  | Оформлення і друк пояснювальної записки |  | *Виконано* |
|  | Оформлення презентації |  | *Виконано* |
|  | Отримання рецензій від рецензента |  | *Виконано* |
|  | Захист в ЕК |  | *Виконано* |

Магістрант О. Бухтіяров

(підпис, дата)

Науковий керівник Н. Гулак

(підпис, дата)

# РЕФЕРАТ

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має \_ сторінок основного тексту, \_ рисунків, \_ таблиць, \_ сторінок додатків. Список використаних джерел містить \_ найменувань і займає \_ сторінок. Загальний обсяг роботи \_ сторінок.

Мета роботи. Для підвищення рівня захищеності інформаційних активів спеціалізованої експертної системи «Портал ESS» удосконалити програмний модуль обліку інформаційних активів за рахунок розробки програмного коду.

В роботі проаналізовано відомості про уразливості, загрози та атаки в інформаційних системах; досліджено методи та засоби управління комплексними системами захисту інформації; розроблено програмний код модуля інвентаризації інформаційних активів.

Розроблений код підвищує рівень захищеності модуля обліку інформаційних активів. В роботі надається порівняльна оцінка підвищення можливості виявлення зовнішнього втручання в інформаційну систему.

Можливі напрямки розвитку цієї роботи пов’язані із додатковими можливостями виявлення несанкціонованого доступу до інформаційних активів підприємств і установ всіх видів власності.

Ключові слова: КІБЕРЗАГРОЗА, АТАКА НА КІБЕРЗАГРОЗУ, ПОРУШНИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ІНФОРМАЦІЙНІ АКТИВИ.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ЗМІСТ** | | | | |
| ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ………………………………………... | | | |  |
| ВСТУП ………………………………………………………………………… | | | |  |
| Розділ 1. АНАЛІЗ НОРМАТИВНИХДОКУМЕНТІВ З СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ……………………………. | | | |  |
|  | 1.1. ISO/IEC 27005:2008 …………………………………………... | | |  |
|  |  | | 1.1.1.Обмеження за стандартом ISO/IEC 27005:2008…… |  |
|  |  | | 1.1.2.Ідентифікація та визначення цінності активів……… |  |
|  |  | | 1.1.3.Оцінки активів організації …………………………... |  |
|  |  | | 1.1.4.Оцінка впливу………………………………………... |  |
|  | 1.2. Класифікація загроз ………………………………… | | |  |
|  | 1.3. Вразливості та методи їх оцінки ……………………... | | |  |
|  | 1.4. Методи оцінки уразливості…………………………………... | | |  |
|  | 1.5. Технічні методи оцінки вразливості ……………... | | |  |
|  | 1.6. Оцінка інформаційних ризиків…………………………………. | | |  |
|  | 1.7. Висновок до розділу …………………………………………….. | | |  |
| Розділ 2. ВИЗНАЧЕННЯ ЦІЛЕЙ ТА ЗАВДАНЬ ПОЛІТИКИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ …………………………………… | | | |  |
|  | 2.1.Основні складові загроз ……………………………………... | | |  |
|  | 2.2. Потенційні загроиз для інформації в ІС ………………………. | | |  |
|  |  | | 2.2.1. Моделі загроз …………………………………… |  |
|  |  | | 2.2.2 Модель порушника …………………………. |  |
|  | 2.3. Ризики для інформаційних активів ………………………... | | |  |
|  | 2.4. Система управління інформаційної безпеки……………….. | | |  |
|  | 2.5. Система менеджменту інформаційної безпеки ……………. | | |  |
|  | 2.6. Висновки до розділу ……………………………………….. | | |  |
| Розділ 3. НАЛАШТУВАННЯ ТА ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМИ | | | |  |
|  | 3.1.Призначення і цілі Системи …………………………………….. | | |  |
|  |  | | 3.1.1. Призначення Системи…… …………………………. |  |
|  |  | | 3.1.2. Цілі створення Системи ……………………. |  |
|  |  | | 3.1.3. Вимоги до структури доступу в Систему ……... |  |
|  | 3.2.Перспективи розвитку і модернізації Системи ………………... | | |  |
|  |  | | 3.2.1.Вимоги до надійності ………………………………… |  |
|  |  | | 3.2.2. Вимоги щодо збереження інформації при аваріях…. |  |
|  |  | | 3.2.3. Вимоги до ергономіки та технічної етіки ………….. |  |
|  |  | | 3.2.4. Вимоги до завдань Системи ………………………… |  |
|  |  | | 3.2.5. Пошук інформації …………………………………… |  |
|  |  | | 3.2.6. Наповнення інформацією Системи ………………… |  |
|  |  | | 3.2.7. Можливість розширення ……………………………. |  |
|  |  | | 3.2.8. Простота впровадження, підтримки і адміністрування ………………………………………………………… |  |
|  | 3.3. Автоматизація модуля інформаційних активів…….………….. | | |  |
|  |  | | 3.3.1.Характеристика об’єкта інформації ………………… |  |
|  |  | | 3.3.2.Автоматизація модуля ……………………………….. |  |
|  |  | | 3.3.3.Опис модуля ………………………………………….. |  |
|  |  | | 3.3.4. Опис рішення реалізації ……………………………. |  |
|  |  | | 3.3.5. Завдання для модуля ………………………………… |  |
|  | 3.4. Етапи та результати виконання проекту ………………………. | | |  |
|  | 3.5.Налаштування системи мониторінгу ІА ……………………….. | | |  |
|  |  | | 3.5.1. Користувач …………………………………………… |  |
|  |  | | 3.5.2. Двухфакторна авторизація ………………………….. |  |
|  |  | | 3.5.3. Головна сторінка …………………………………….. |  |
|  |  | | 3.5.4. Редагування вразливості …………………………….. |  |
|  |  | | 3.5.5. Створення нової групи активів ……………………... |  |
|  |  | | 3.5.6. Редагування вразливості …………………………….. |  |
|  |  | | 3.5.7. Розділ «Інцидент» …………………………………… |  |
|  |  | | 3.5.8. Розділ «Інформаційні активи» |  |
|  | 3.6. Опис модуля «Інформаційні активи» ………………………….. | | |  |
|  | 3.7.Оцінка ефективності розробленого коду ………………………. | | |  |
|  | 3.8. Висновок по розділу ……………………………………………. | | |  |
| ВИСНОВКИ …………………………………………………………………... | | | |  |
| СПИСОК ВИКОРИСТАНОЇ ДЖЕРЕЛ ……………………………………... | | | |  |
| Додаток А. | | Програмний продукт коду …..………………………………... | |  |

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Модель ПВПД - (плануй-виконуй-перевіряй-дій; англ. Plan-Do-Check-Act, PDCA)

СУІБ - Система управління інформаційною безпекою

ІА – інформаційні активи

ORM– это аббревиатура для Object Relational Mapping (Объектно-реляционное отображение).

# ВСТУП

**Актуальність**. Повсюдне впровадження сучасних інформаційних технологій передбачає поряд з раціональним використання ресурсів розподіленої комп'ютерної мережі ще й організацію ефективної протидії загрозам нападу на її інфраструктуру. Безперервні зміни в конфігурації системи, її параметрів і складу програмного забезпечення вимагають постійного аналізу стану захищеності системи, передбачення і виявлення нових загроз безпеці і застосування превентивних заходів.

Сьогодні, поряд з інтеграцією функціональної, схемотехничної, мережевої, активно розвивається інтегральна безпека, що характеризує такий стан життєдіяльності людини, а також функціонування об'єктів і інформації, при якому вони надійно захищені від усіх можливих видів загроз в ході безперервного життєвого процесу і вирішення поставлених завдань.

Сучасні інформаційні технології не тільки автоматизують основні функції діяльності підприємств (організацій, установ), тим самим сприяючи досягненню цілей діяльності, але й можуть надати їм ряд нових затребуваних функцій та сервісів. Це означає, що інформаційні технології стають активами підприємства і, як будь-які активи, вимагають управління, спрямованого на мінімізацію ризиків його діяльності [1].

Інформаційна безпека являє собою сукупність процесів, спрямованих у тому числі на мінімізацію ризиків інформаційних технологій і, як наслідок, мінімізацію ризиків діяльності підприємства. Кінцевою метою безпеки є забезпечення стану захищеності інтересів і мети діяльності підприємства.

Для успішного використання сучасних інформаційних технологій необхідне надійне та ефективне управління не тільки власне інформаційними системами, але і засобами їх безпеки. Якщо у минулому завдання полягало в забезпеченні управління окремими засобами (наприклад, серверами, мережами та маршрутизаторам), то зараз виникає необхідність забезпечити інформаційну безпеку корпоративних процесів діяльності підприємств.

У зв'язку з цим на перший план виступає завдання створення комплексної системи управління, яка охоплює всю інфраструктуру підприємства і, незалежно від складності та масштабу інформаційної системи, що дозволяє:

-централізовано та оперативно здійснювати управляючі впливина всю інформаційну інфраструктуру;

-проводити регулярний аудит та всеохоплюючий моніторинг, що дає об'єктивну інформацію про стан інформаційної безпеки для прийняття оперативних рішень;

- проводити збір статистичних даних про роботу інформаційної інфраструктури для прогнозування її розвитку.

**Відомі підходи до вирішення поставленої задачі.** Вирішення завдань для прийняття оперативних рішень при виявленні в процесі моніторингу порушень інформаційної безпеки (ІБ) можливо за допомогою створення спеціалізованих експертних систем для досягнення максимальної синергії та консолідації в системі менеджменту інформаційної безпеки (СМІБ).

Другим підходом до вирішення завдань СМІБ є інтегральна безпека. Інтегральна безпека в межі акумулює в собі всі необхідні для вирішення даного завдання види безпеки (охоронна, пожежна, екологічна, особиста, інформаційна тощо). Поняття інтегральної безпеки передбачає обов'язкову безперервність процесу забезпечення безпеки, як в часі, так і в просторі по всьому технологічному циклу діяльності з обов'язковим урахуванням усіх можливих видів загроз (витоку інформації, несанкціонованого доступу, тероризму, пожежі, аварій, і т.п.). Тому, наприклад, при забезпеченні інтегральної безпеки організації, фірми, будь-якої комерційної структури в обов'язковому порядку повинні враховуватися одночасно питання, як забезпечення інформаційної безпеки, так і захисту об'єкта і персоналу [2].

**Мета роботи** полягаєв удосконаленні програмного модулю для підвищення рівня захищеності інформаційних активів спеціалізованої експертної системи «Портал ESS».

Для досягнення поставленої мети вирішуються такі **задачі:**

* проведення аналізу систематизованої сукупності відомостей про уразливості, загрози та атаки в інформаційних системах;
* дослідження методів та засобів управління комплексними системами захисту інформації;
* розробка програмного коду модуля інвентаризації інформаційних активів та оцінка підвищення рівня його захищеності.

**Галузь застосування**. Розроблений програмний продукт відноситься до галузі кібербезпеки і підвищує ефективність роботи СМІБ, що призводить до додаткового економічного ефекту

**Об’єктом дослідження** є процес моніторингу порушень ІБ для проведення заходів з удосконалення СМІБ.

**Предметом дослідження** є основні модулі роботи спеціалізованих експертних систем.

**Методи дослідження:** методи математичної статистики, методи оцінки ризиків, методи управління інформаційної безпеки, об’єктно-орієнтоване програмування (мова програмування Java).

**Новизна одержаних результатів полягає в наступному:**

впровадження спеціалізованої експертної системи «Портал ESS» (розробник Україна) до якої входить модуль інвентаризації інформаційних активів, істотно підвищує функціональні здатності для рішень, та вперше виключають використання неуніфікованих та затратних процесів підготовки, узгодження, затвердження та реалізації, які використовуються в процесах управління СМІБ.

**Практичне значення отриманих результатів:**

розроблений програмний код для модуля інвентаризації інформаційних активів дає додаткові можливості виявлення несанкціонованого доступу до інформаційних активів підприємств і установ всіх видів власності та підвищує рівень їх захищеності.

# Розділ 1. Аналіз нормативних документів з системи менеджменту інформаційної безпеки

Для успішного використання сучасних інформаційних технологій необхідне надійне та ефективне управління не тільки інформаційними системами, але і засобами їх безпеки, тому зараз виникає необхідність забезпечити інформаційну безпеку корпоративних процесів діяльності підприємств.

**1.1.Огляд стандартів з управління інформаційної безпеки**

Група стандартів ISO / IEC 27000 є загальновизнаним світовим еталоном з організації управління інформаційною безпекою. Частиною групи є стандарти ISO/IEC 27001 «Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації. Вимоги » та ISO / IEC 27002 « Інформаційні технології. Звід правил по управлінню захистом інформації ». Перший стандарт має аналог ГОСТ ISO / IEC 27001. Другий міжнародний стандарт має прототип у вигляді британського стандарту BS 7799 (Практичні правила управління інформаційною безпекою), який був повністю перенесено в опублікований організаціями ISO і IEC міжнародний стандарт ISO / IEC 17799: 2 000 «Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки ". На основі даного стандарту був прийнятий стандарт ГОСТ РІСО/МЕК 17799-2005 Інформаційна технологія. Практичні правила управління інформаційною безпекою. У 2007 році ISO і IEC взамін ISO / IEC 17799: 2000 був опублікований стандарт ISO / IEC 27002: 2005 «Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки ". У новому стандарті є деякі відмінності від прототипу, але вони не принципові, а суть підходу до організації ІБ змінилася. Для зручності та однозначності будемо посилатися на стандарти ISO 27001 та ISO 27002. По суті, стандарт ISO 27001 визначає підходи і структуру управління ІБ, а стандарт ISO 27002 - деталізує вимоги до категорій СОІБ.

Слід згадати ще один стандарт, що входить до групи Стандарт ISO/IEC 27000 - ISO/IEC 27005 (Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки). Так як область управління ризиками ІБ, хоч і лежить в основі організації всієї групи стандартів ISO 27000, є дуже специфічною, і тому потребує окремого анали за. Згадані стандарти визначають конструкцію системи ІБ, до якої треба прагнути при її створенні і розвитку.

**1.1.1.Обмеження за стандартом ISO/IEC 27005:2008**

В стандарті ISO/IEC 27005:2008 надані рекомендації для менеджменту риска ІБ в установах, фірмах, підприємствах, тощо.

Для створення й ефективного функціонування системи менеджменту інформаційної безпеки необхідно визначити області застосування і межі процесу менеджменту ризиків ІБ [3].

Дослідження організації представлено в таблиці 1.1.

Таблиця 1.1.

Параметри дослідження організації

|  |  |
| --- | --- |
| Параметр дослідження | Зміст параметру |
| 1. | 2. |
| Оцінка організації | Дослідження організації виявляє характеристики елементів, що ідентифікують організації. Це стосується намірів, бізнесу, місій, значень і стратегій цієї організації. Вони повинні бути ідентифіковані разом з елементами їх розробки (наприклад, висновок субпідрядної договору). Труднощі цієї діяльності полягає в точному розумінні як структурована організація. Ідентифікація еѐ реальної структури забезпечить розуміння ролі і важливості кожного підрозділу в досягненні цілей організації. |
| Продовження таблиці 1.1. | |
| 1. | 2. |
| Основні наміри організації | Основні наміри організації можуть бути визначені як мотив, навіщо вона існує (її поле діяльності, її ринковий сегмент, тощо). |
| Бізнес організації | Бізнес організації, що визначається службовцями і методиками ноу-хау дає можливість досягти своєї місії. Це є визначальним для поля діяльності організації . |
| Місія організації | При досягненні організацією своїх намірів досягається її місія. Щоб ідентифікувати місію повинні бути ідентифіковані надані послуги та / або виготовлені продукти відносно кінцевих користувачів. |
| Значення організації | Головний принцип значень - читкий кодекс поведінки ставився до здійснення бізнесу. Це може торкнутися персоналу, відносин із зовнішніми агентами (клієнтами, тощо), якістю продуктів або наданих послуг. |
| Структура організації | 1.дрібна структура: кожен розділ знаходиться під владою менеджера підрозділу, відповідального за стратегічні, адміністративні та оперативні рішення щодо його модуля;  2. функціональна структура: функціональна влада здійснена на процедурах, природі роботи і іноді рішень або планування (наприклад, продукція, IT, людські ресурси, маркетинг і т.д.); |
| Організаційна структура | Структура організації представлена схематично в організаційній структурі. Це подання має виділити направлення повідомлень і делегацію повноважень, але  має також включати інші відносини, які навіть якщо вони не засновані на формальних повноважень є, проте, напрямками потоку інформації. |
| Стратегія організації | Це вимагає формального вираження керівних принципів організації. Керівництво визначає стратегію організації і необхідну розробку, щоб витягти вигоду з проблем загроз і планованих головних змін |

Для здійснення комплексу дій, спрямованих на управління системою менеджменту інформаційної безпеки шляхом уніфікації і підвищення ефективності процесів ІБ необхідно читко визначити обмеження, що зачіпають організацію і визначають орієнтацію її інформаційної безпеки [3]. Список обмежень наведено в таблиці 1.2.

Організація встановлює свої цілі, що фіксуються до конкретної мети. Ця ціль може бути виражена як стратегія дії або розробки з ціллю зменшення експлуатаційних витрат, покращення якості сервісу, тощо.

Таблиця 1.2.

Перелік обмежень при виборі СМІБ

|  |  |
| --- | --- |
| Тип обмеження | Причини обмеження |
| 1. | 2. |
| Обмеження політичної природи | Вони можуть торкнутися урядових адміністрацій, громадських установ або в ширшому розумінні будь-якої організації, яка повинна застосовувати урядові рішення. Це рішення зазвичай відносно стратегічною або оперативної орієнтації, які повинні бути застосовані підрозділом урядових органів для прийняття рішень. |
| Обмеження стратегічної природи | Обмеження можуть з'явитися результатом запланованих або можливих змін до структур організації або орієнтації. Вони виражені в стратегічних або оперативних планах організації. |
| Територіальні обмеження | Структура організації і / або мета можуть ввести визначені обмеження, такі як розподіл сайтів по всій національній території або за кордоном. |
| Обмеження, що є результатом економічного та політичного клімату | Операційна діяльність організації може бути глибоко змінена специфічними подіями, такими як потрясіння або національні та міжнародні кризи |
| Структурні обмеження | Природа структури організації (дробової, функціональної або інший) може привести до певної організаційної політики безпеки і організації безпеки, адаптованої до структури. |
| Функціональні обмеження | Функціональні обмеження виникають безпосередньо із загальних або певної місій організації. |
| Обмеження відносно персоналу | Природа цих обмежень значно змінюється. Вона пов'язана з: рівнем відповідальності, кваліфікацією, навчанням, розумінням безпеки, доступністю, тощо. |
| Продовження таблиці 1.2. | |
| 1 | 2 |
| Обмеження, що виникають в результаті реєстрації організації | Ці обмеження можуть слідувати з реструктурування або установки нової національної або міжнародної політики, накладає певні обмеження. |
| Обмеження, що пов’язані з методами | Методи, відповідні ноу-хау організації повинні будуть бути накладені для планування, специфікації, тощо. |
| Обмеження культурної природи | Деякі звички роботи в організації привели до певної "культури" в межах організації, яка може бути несумісна з менеджментом безпеки. Ця культура - загальна структура довідкової інформації персоналу і можна визначити багатьма аспектами, включаючи освіту, машинну команду, професійний досвід, т.д. |
| Бюджетні обмеження | У рекомендованих контролів безпеки може іноді бути дуже висока вартість. Не завжди доречно будувати інвестиції безпеки на рентабельності, фінансовим підрозділом організації взагалі потрібно економічного виправдання. |
| Обмеження, що є результатом існуючих раніше процесів | Прикладні проекти не обов'язково розроблені одночасно. Деякі залежать від існуючих раніше процесів. Навіть при тому, що процес може бути розподілений на підпроцеси, процес не обов’язково знаходиться під впливом всіх підпроцесів іншого процесу. |
| Технічні обмеження | Технічні обмеження взагалі є результатом встановлених апаратних засобів, програмного забезпечення, ділянок пам'яті або сайтів, що поміщають процеси:  файлів; загальної архітектури; прикладного програмного забезпечення; упаковки програмного забезпечення; апаратних засобів; мереж комунікації; інфраструктур які вбудовуються. |
| Фінансові обмеження | Реалізація контролів безпеки часто обмежується бюджетом. Однак, фінансове обмеження, яке розглянуть, має всі ще бути продовженим, оскільки про розподіл бюджету для безпеки можна домовитися на основі дослідження безпеки. |
| Продовження таблиці 1.2. | |
| 1 | 2 |
| Екологічні обмеження | Екологічні обмеження є результатом географічної або економічної обстановки, в якій здійснені процеси: країна, клімат, природні ризики, географічна ситуація, економічний клімат і т.д. |
| Часові обмеження | Потрібно розглянути час, необхідний для того, щоб здійснити менеджмент безпеки, щодо спроможності модернізувати інформаційну систему; якщо час реалізації дуже тривалий, ризики для яких був спроектований менеджмент, можливо, зміниться. Час - коефіцієнт визначення для того, щоб вибрати рішення і пріоритети. |
| Обмеження за методами | Методи, відповідні ноу-хау організації, повинні використовуватися для проектного планування, специфікацій, розробка і так далі. |

**1.1.2. Ідентифікація та визначення цінності активів**

Щоб визначити цінність активу, організація спочатку повинна здійснювати ідентифікацію свої активи (на відповідному рівні деталізації) [3]. Можна відрізнити два види активів які представлені на рисунку 1.1.

Зазвичай первинні активи - це основні процеси та інформаційна діяльність в області застосування. Можна також розглядати інші первинні активи, такі як процеси всередині організації, які будуть більш відповідними для складання політики інформаційної безпеки або плану безперервності бізнесу. Залежно від мети деякі дослідження не вимагатимуть вичерпного аналізу всіх елементів, складових сферу застосування.



Рис. 1.1. Види активів

У таких випадках межі дослідження можуть бути обмежені ключовими елементами області застосування[3].

Типи первинних активів представлені в таблиці 1.3.

Таблиця 1.3.

Типи та зміст первинних активів

|  |  |
| --- | --- |
| Тип активу | Зміст активу |
| Бізнес-процеси | -це втрата або деградація активу, що позбавляють можливості виконувати місію організації;  - які містять секретні процеси або процеси, що залучають приватну;  технологію;  - які, якщо змінені, можуть сильно зачепити виконання місії;  організації;  - які необхідні для організації, щоб виконати договірні,  юридичні або регулюють вимоги. |
| Продовження таблиці 1.3. | |
| 1. | 2. |
| Інформація | Більш широко, первинна інформація включає головним чином:  - життєво важливу інформацію для здійснення місії або бізнесу;  - персональну інформацію, яка може бути визначена державою щодо права приватного життя;  - стратегічну інформацію для досягнення цілей, що визначається стратегічними орієнтаціями;  - інформацію високу вартість на збір якої, зберігання, обробку та передачу потрібно багато часу і / або залучення високих фінансових витрат. |

**1.1.3. Оцінки активів організацій.**

В кінцевому аналізі повинні бути ретельно визначені, оцінені або призначені значення на актив, так як кінцеве призначений значення виступає в визначення ресурсів, які будуть витрачені для захисту активу.

Критерії, які можуть використовуватися, щоб оцінити можливі наслідки представлені на рисунку 1.2. Критерії поділяються на два типа:

1.критерії з втрати конфіденційності, цілісності, доступності, неможливість відмови від авторства, спостережливості, автентичності або надійності активів;

2. критерії оцінки наслідків.



Рис. 1.2. Типи критеріїв оцінки збитків

Ці критерії - приклади проблем, які розглядаються для оцінки активу. Для того щоб виконати оцінки, організація повинна вибрати критерії, які стосуються її типу вимог безпеки і бізнесу.

**1.1.4. Оцінка впливу**

Інцидент інформаційний безпеки може впливати на більше ніж один актив або тільки частина активу. Вплив пов'язано певною мірою успіху інциденту. Як наслідок, є суттєва відмінність між значенням активу і впливом, що випливають з інциденту. Впливом вважають наявність або безпосередній (експлуатаційний) ефект або майбутній (бізнес) ефект, який включає фінансові та ринкові наслідки. Безпосереднє (експлуатаційне) вплив є прямим або непрямим. Зміст цих впливів наведено на рисунку 1.3 [3].

Рис. 1.3. Оцінки впливу.

**1.2.Класифікація загроз.**

Загрози можуть бути навмисними, випадковими або екологічними (природними) і мати результат, наприклад, порушення або втрата основних сервісів. Наступний список показує релевантні для кожного типу загрози, де D (навмисні), А (випадкові елемент), E (екологічні). D використовується для всіх навмисних акцій, націлених на інформаційні активи, A використовується для всіх людських дій, які можуть випадково пошкодити інформаційні активи і E використовується для всіх інцидентів, які не засновані на людських діях (табл.1.4). Групи загроз не знаходяться в пріоритетному порядку [3].

Таблиця 1.4.

Класифікація загроз

|  |  |  |
| --- | --- | --- |
| Тип | Загрози | Позначення |
| 1. | 2. | 3. |
| Фізичне пошкодження | Вогонь | A,D,E |
| Пошкодження водою | A,D,E |
| Забруднення | A,D,E |
| Значний інциндент | A,D,E |
| Знищення обладнання або носіїв | A,D,E |
| Пил, корозія, обмерзання | A,D,E |
| Природні події | Кліматичні явища | Е |
| Сейсмічні явища | Е |
| Вулканічні явища | Е |
| Метеорологічні явища | Е |
| Повінь | Е |
| Втрата необхідних сервісів | Відмова кондиціону-вання та водопостачання | A,D |
| Втрачання електроенергії | A,D,E |
| Відмова телекомунікаційного обладнення | A,D |
| Радіаційні несправності | Електромагнітна радіація | A,D,E |
| Теплова радіація | A,D,E |
| Електромагнітний імпульс | A,D,E |
| Компрометація інформації | Перехоплення і відправка компрометувати сигналу | D |
| Віддалений шпіонаж | D |
| Підслуховування | D |
| Крадіння носіїв або документів | D |
| Крадіння обладнання | D |
|  |  |  |
| Продовження таблиці 1.4. | | |
| 1. | 2. | 3. |
| Компрометація інформації | Відновлення інформації на носіях, відправлених на переробку або бракованих | D |
| Виявлення | A,D |
| Дані з ненадійних джерел | A,D |
| Втручання в апаратні засоби | D |
| Втручання в програмні засоби | D |
| Виявлення позицій | D |
| Технічні відмови | Відмова обладнання | А |
| Збій обладнання | А |
| Обмеження інформаційної системи | A,D |
| Програмний збій | А |
| Порушення ремонтопридатності інформаційної системи | A,D |
| Несанкціоновані дії | Несанкціоноване використання обладнення | D |
| Шахрайське копіювання  програмного забезпечення | D |
| Використання підробленого або скопійованого програмного забезпечення | A,D |
| Спотворення даних | D |
| Незаконна обробка даних | D |
| Компрометація функцій | Помилка в використанні | А |
| Зловживання правами | A,D |
| Підробка прав | D |
| Заперечення дій | D |

Особливу увагу потрібно звернути на людський фактор, який відігріває не останню роль як джерело загрозі інформації (табл. 1.5.) [3].

Таблиця 1.5.

Мотивація людських загроз

|  |  |  |
| --- | --- | --- |
| Джерело загрози | Мотивація | Можливі наслідки |
| Хакер, крекер | Повстання  Его  Визов  Статус  Гроші | Хакерство  Соціальна інженерія  Вторгнення в систему, порушення  Несанкціонований доступ в систему |
| Комп’ютерний злочинець | Руйнування інформації  Незаконне розкриття  інформації  Грошово-кредитна вигода  Неправомірне  чергування даних | Комп'ютерний злочин  (наприклад, кібер-переслідування)  Шахрайське дія  (наприклад, перегравання,  наслідування, перехоплення)  Інформаційне хабарництво  Імітація  Вторгнення в систему |
| Терорист | Помста  Розвідка  Руйнування  Шантаж  Політичні вигоди  Освітлення в пресі | Бомба / Тероризм  Інформаційна війна  Системна атака (наприклад,  розподілена відмова в  обслуговуванні)  Проникнення в систему  Втручання в систему |
| Індустріальне шпигунство (компанії, іноземні уряди, інші  урядові інтереси) | Розвідка  Его  Цікавість  Грошово-кредитна вигода  Помста  Ненавмисні помилки і  Упущення | Вторгнення в систему  Перегляд секрету фірми  Інформаційне хабарництво  Введення фальсифікованих  даних, руйнування даних  Перехоплення  Шкідливий код  Несанкціонований  доступ в систему |

В наступному підрозділі буде розглянуто вразливості ІБ.

**1.3. Вразливості та методи їх оцінки.**

Людський фактор є одним з слабких ланок, тому що піддається емоціям та має багато спокус. Людські джерела загрози відповідно перераховані в таблиці 1.6.[3]:

Таблиця 1.6.

Фактори людських загроз

|  |  |  |
| --- | --- | --- |
| Джерело загроз | Мотивація | Можливі наслідки |
| 1. | 2. | 3. |
| Хакер, крекер | Повстання  Его  Виклик  Статус  Гроші | Хакерство  Соціальна інженерія  Вторгнення с систему, порушення  Несанкціонований доступ в систему |
| Комп’ютерний злочинець | Порушення інформації  Незаконне розкриття інформації Грошово-кредитна вигода  Неправомочне чередування да-них | Комп'ютерний злочин Шахрайська дія Інформаційне хабарництво Імітація, вторгнення в систему |
| Терорист | Помста  Розвідка  Руйнування  Шантаж  Політичні вигоди  Освітлення у пресі | Бомба/Тероризм Інформаційна війна Системна атака (наприклад, розподілѐна відмова в обслуговуванні) Проникнення в систему Втручання в систему |
| Індустріальне шпигунство (компанії, іноземні уряди, інші урядові інтереси) | Конкурентоздатна перевага Економічне шпигунство | Економічна розвідка Інформаційна крадіжка Вторгнення в персональні дані  Соціальна розробка Проникнення в систему Несанкціонований доступ в систему (доступ до секретної, приватної, і/або пов'язаній з технологією інформації) |
| Продовження таблиці 1.6. | | |
| 1. | 2. | 3. |
| Інсайдер (погано навчені, розсерджені, зловмисні, недбалі, нечесні або звільнені службовці) | Розвідка  Его  Цікавість  Грошово-кредитна вигода Помста  Ненавмисні помилки і упущення (наприклад, помилка введення даних, помилка програмування) | Напад на службовця Шантаж  Перегляд секрету фірми Неправильне комп'ютерне поводження  Шахрайство і крадіжка Інформаційне хабарництво Введення фальсифікованих даних, руйнування даних  Перехоплення  Шкідливий код (наприклад, вірус, логічна бомба, троян-ський кінь)  Продаж персональної інформації  Системні помилки Вторгнення в систему Системний саботаж  Несанкціонований доступ в систему |

**1.4. Методи для оцінки уразливості**

У [комп'ютерній безпеці](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0), уразливість ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *system vulnerability*) — нездатність системи протистояти [реалізації](https://uk.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D0%B0_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) певної [загрози](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0) або сукупності загроз [4]. Тобто, це певні недоліки в комп'ютерній системі, завдяки яким можна навмисно порушити її цілісність і викликати невірну роботу.

Уразливість може виникати в результаті допущених помилок [програмування](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F), недоліків, допущених при проектуванні системи, ненадійних паролів, вірусів та інших шкідливих програм, скриптових і [SQL-ін'єкцій](https://uk.wikipedia.org/wiki/SQL_%D1%96%D0%BD%27%D1%94%D0%BA%D1%86%D1%96%D1%8F). Деякі уразливості відомі тільки теоретично, інші ж активно використовуються і мають відомі [експлойти](https://uk.wikipedia.org/wiki/%D0%95%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82).

Наведемо приклади вразливості в різних областях безпеки включаючи приклади загроз, які могли б експлуатувати цю уразливість. Перелік може забезпечити довідку під час оцінки загроз і уразливості, визначити відповідні інцидентні сценарії (табл.1.7.). В деяких випадках інші загрози можуть експлуатувати також цю уразливість [3].

Таблиця 1.7.

Приклади вразливості та загроз

|  |  |  |
| --- | --- | --- |
| Тип | Приклад вразливості | Приклади загроз |
| 1. | 2. | 3. |
| Апаратні засоби | Недостатнє обслуговування / дефектна інсталяція з носіїв даних | Пролом в ремонтопридатності інформаційної системи |
| Вади схем для періодичних замін | Руйнування устаткування або носіїв |
| Сприйнятливість до вологості, пилу, забрудненню | Пил, корозія, обмерзання |
| Чутливість до електромагнітної радіації | Електромагнітна радіація |
| Вади ефективного контролю внесення змін конфігурації | Помилка у використанні |
| Сприйнятливість до змін напруги | Втрата джерела живлення |
| Сприйнятливість до температурних змін | Метеорологічне явище |
| Апаратні засоби | Незахищіне зберігання | Крадіжка носіїв або документів |
| Недолік в обережності при знищенні | Крадіжка носіїв або документів |
| Неконтрольоване копіювання | Крадіжка носіїв або документів |
| Програмне забезпечення | Відсутність або недостатнє програмне тестування | Зловживання правами |
| Відомі недоліки в програмному забезпеченні | Зловживання правами |
| Немає виходу з системи при залишенні робочої станції | Зловживання правами |
| Передача або багатократне використання носіїв даних без належного стирання | Зловживання правами |
| Передача або багатократне використання носіїв даних без належного стирання | Зловживання правами |
| Мале число ревізій | Зловживання правами |
| Неправильний розподіл прав доступу | Зловживання правами |
| Продовження таблиці 1.7. | | |
| 1. | 2. | 3. |
| Програмне забезпечення | Широко розповсюджене програмне забезпечення | Спотворення даних |
| Застосування застосовних програм до фальшивих даних в термінах часу | Спотворення даних |
| Складний призначений для користувача інтерфейс | Помилка у використанні |
| Вади в документуванні | Помилка у використанні |
| Встановлено невірний параметр | Помилка у використанні |
| Некоректні дати | Помилка у використанні |
| Широко розповсюджене програмне забезпечення | Спотворення даних |
| Мережа | Вади ідентифікуючих і розпізнавальних механізмів для призначеної для користувача аутентифікації | Підробка прав |
| Незащищѐнные таблиці паролів | Підробка прав |
| Поганий менеджмент паролями | Підробка прав |
| Запущені непотрібні служби | Незаконна обробка даних |
| Недопрацьоване або нове програмне забезпечення | Програмний збій |
| Мережа | Неясні або неповні специфікації для розробників | Програмний збій |
|  | Вада ефективний контролю внесення зміна | Програмний збій |
|  | Неконтрольоване завантаження і використання програмного забезпечення | Підробка програмного забезпечення |
|  | Вади в процедурі резервного копіювання | Підробка програмного забезпечення |
|  | Вади фізичного захисту будівлі, дверей і вікон | Крадіжка носіїв або документів |
|  | Відмова менеджменту від перевірки звітів | Несанкціоноване використання устаткування |
|  | Нестача доказу посилки або отримання повідомлення | Заперечення дій |
| Продовження таблиці 1.7. | | |
| 1. | 2. | 3. |
|  | Незахищена лінія зв'язку | Підслуховування |
|  | Незахищений чутливий трафік | Підслуховування |
|  | Погана спільна проводка | Відмова телекомунікаційного устаткування |
|  | Єдина точка відмови | Відмова телекомунікаційного устаткування |
|  | Вади ідентифікації і аутентифікація відправника і одержувача | Підробка прав |
|  | Небезпечна мережева архітектура | Віддалене шпигунство |
|  | Передача паролів у відкритому виді | Віддалене шпигунство |
|  | Неадекватний менеджмент мережею (здатність системи протистояти помилкам маршрутизації) | Насиченість інформаційної системи |
|  | Незащищѐнные підключення загальнодоступної мережі | Несанкціоноване використання устаткування |
| Персонал | Відсутність персоналу | Порушення доступності персоналу |
| Неадекватні процедури вербування | Знищення устаткування або носіїв недостатнє навчання безпеки |
| Помилка у використанні неправильне використання програмного забезпечення | Помилка у використанні |
| Персонал | Вади розуміння безпеки | Помилка у використанні |
| Нестача механізмів моніторингу | Незаконна обробка даних |
| Неконтрольована робота зовнішнім штатом або персоналом що прибирає | Крадіжка носіїв або документів |
| Вада політики для вірного використання носіїв передачі даних і обміну повідомлень | Несанкціоноване використання устаткування |
| Сайт організації | Неадекватне і недбале використання фізичного контролю доступу до будівлі і приміщень | Знищення устаткування або носіїв інформації |
| Продовження таблиці 1.7. | | |
| 1. | 2. | 3. |
| Сайт організації | Місце розташування в області, сприйнятливій до затоплення | Нестабільна потужність мережі |
| Повінь | Втрата джерела живлення |
| Нестача фізичного захисту створення, дверей і вікон | Крадіжка устаткування |
| Вади формальної процедури для призначений для користувача реєстрації і де-регистрації | Зловживання правом |
| Вади формального процесу для перегляду права доступу (диспетчерський менеджмент) | Зловживання правом |
| Дефіцит або недостатні умови (відносно безпеки) в контрактах з клієнтами і/або третіми особами м | Зловживання право |
| Вади в процедурі для контролю над засобами обробки інформації ом | Зловживання прав |
| Вади регулярних ревізій (диспетчерський менеджмент) | Зловживання правом |
| Нестача процедур виявлення ризику і оцінки | Зловживання правом |
| Недостатність інформації в записі звітів про несправність ужурналі адміністратору і користувача | Зловживання правом |
| Неадекватна відповідь обслуговуючого сервісу | Порушення ремонтопридатності інформаційної системи |
| Вади або недостатня угода сервісного обслуговування | Порушення ремонтопридатності інформаційної системи |
| Вади процедури контролю внесення змін | Порушення ремонтопридатності інформаційної системи |
| Вади формальної процедури для менеджменту документацією СМІБ | Спотворення даних |
| Вади формальних процедур записів для СМИБ, які робить диспетчерський менеджмент | Спотворення даних |
| Вада формального дозволу для процесу загального доступу | Інформація даних з ненадійного джерела |
| Продовження таблиці 1.7. | | |
| 1. | 2. | 3. |
|  | Вада належний розподіл обов'язок інформаційний безпека | Заперечення дій |
|  | Вади планів безперервності | Відмова устаткування |
|  | Вади політики використання поштової скриньки | Помилка у використанні |
|  | Нестача процедур для того, щоб ввести програмне забезпечення в експлуатовані системи | Помилка у використанні |
|  | Нестача звітів у файлах реєстрації адміністратора і оператора анні | Помилка у використ |
|  | Нестача процедур для обробки секретних даних | Помилка у використанні |
|  | Вади обов'язків інформаційної безпеки в описах завдань | Помилка у використанні |
|  | Вади або недостатні умови (відносно інформаційній безпеки) в контрактах із службовцями | Незаконна обробка даних |
|  | Нестача визначеного дисциплінарного процесу у разі інформаційного інциденту безпеки | Крадіжка устаткування |
|  | Нестача формальної політики по використанню мобільної комп'ютерної техніки | Крадіжка устаткування |
|  | Нестача менеджменту активів дистанційного резервування | Крадіжка устаткування |
|  | Нестача або недостатня політика "чистого столу і чистого екрану" | Крадіжка носіїв або документів |
|  | Нестача санкцій на засоби обробки інформації | Крадіжка носіїв або документів |
|  | Нестача встановлених контрольних механізмів у разі порушень правил безпеки | Крадіжка носіїв або документів |
|  | Нестача регулярних переглядів / контролей | Несанкціоноване використання устаткування |
|  | Нестача процедури для того, щоб повідомити про уразливість безпеки | Несанкціонований використання устаткування |

Зазвичай уразливість дозволяє атакуючому «обдурити» додаток — змусити його вчинити дію, на яку у нього не повинно бути прав. Це робиться шляхом впровадження будь-яким чином в програму даних або коду в такі місця, що програма сприймала їх як «свої». Деякі уразливості з'являються через недостатню перевірку даних, що вводяться користувачем і дозволяють вставити в інтерпретований код довільні команди ([SQL](https://uk.wikipedia.org/wiki/SQL)-ін'єкція, [XSS](https://uk.wikipedia.org/wiki/XSS)). Інші уразливості з'являються через більш складні проблеми, такі як запис даних в [буфер](https://uk.wikipedia.org/wiki/%D0%91%D1%83%D1%84%D0%B5%D1%80) без перевірки його меж (переповнення буфера) [5].

Отже, основними причинамивразливостей є:

Складність: великі, складні системи збільшують ймовірність дефектів і ненавмисних точок доступу [5].

Відомість: використання загального, відомого коду, [програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F), операційних систем та/або обладнання збільшує ймовірність того, що зловмисник може знайти інформацію та інструменти, щоб використати недолік [6].

Зв'язок: фізичні з'єднання, привілеї, порти, протоколи, служби та час, який вони є доступними, збільшує вразливість.

Недостатній контроль паролів: користувач використовує слабкі паролі, які можуть бути виявлені за допомогою грубої сили; користувач комп'ютера зберігає пароль на комп'ютері, на якому програма може отримати до нього доступ; користувач повторно використовує паролі між багатьма програмами і веб-сайтами [5].

Фундаментальні недоліки дизайну операційної системи: дизайнер [операційної системи](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) вибирає для забезпечення роботи неоптимальні політики управління «користувач — програма». Наприклад, операційні системи з політикою щодо дозвілу на отримання повного доступу до всього комп'ютера для будь якої програми чи користувача. Ці недоліки операційної системи дозволяють вірусам і шкідливим програмам виконувати команди від імені адміністратора [6].

Перегляд веб-сайту: Деякі сайти можуть містити шкідливі шпигунські або рекламні програми, які можуть бути автоматично встановлені на комп'ютерних системах. Після відвідування цих сайтів, комп'ютерні системи можуть заразитися і особиста інформація буде збиратися і передаватися до сторонніх осіб [7].

[Помилки програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%91%D0%B0%D2%91): Програміст залишає помилку в програмі, яка може дозволити зловмиснику зловживати программою [5].

Необмежений вхід користувача: Програма припускає, що все, що вводить користувач безпечно. Програми, які не перевіряють введення користувача, можуть дозволити ненавмисне безпосереднє виконання команд або операторів SQL (відомих як переповнення буфера, ін'єкції SQL та інші неперевірені входи) [5].

**1.5 Технічні методи оцінки вразливості**

Щоб ідентифікувати уразливості залежно від критичності інформації і інформаційно-комунікаційних технологій (ICT) можуть використовуватися превентивні методи, такі як тестування інформаційної системи, системних і доступних ресурсів (наприклад, розподіленні фонди, доступні технології, проведення тесту людей-експертів). Випробувальні методи включають [3]:

- автоматизований інструмент сканування вразливостей;

- тестування безпеки і оцінку;

- тестування проникнення;

- перегляд коду.

Щоб проглянути групу головних комп'ютерів або мережу на предмет відомих вразливих служб (наприклад, систему, що дозволяє анонімний протокол передачі файлів (FTP), передачу sendmail), використовується автоматизований інструмент сканування вразливості. Проте треба відмітити, що частина потенційних вразливостей, ідентифікованих автоматизованим інструментом сканування, представляє реальну уразливість в контексті системного середовища[3].

Тестування безпеки і оцінка є іншою методикою, яка може використовуватися в ідентифікації уразливості системи ICT під час процесу оцінки ризику. Це включає розробку і виконання плану випробувань (наприклад, випробувальний скрипт, випробувальні процедури і очікувані результати випробувань). Мета системного тестування безпеки полягає в тому, щоб перевірити ефективність контролей безпеки системи ICT, оскільки вони були застосовані в експлуатованому середовищі. Мета полягає в тому, щоб гарантувати, що менеджмент використовує схвалену специфікацію безпеки для прикладного програмного забезпечення і устаткування і здійснюють політику безпеки організації або використовує галузеві стандарти [3].

Може використовуватися тестування проникнення, щоб доповнити перегляд контролей безпеки і гарантувати, що забезпечені різні аспекти системи ICT. Коли застосовується тестування проникнення в процесі оцінки ризику, результати цього можуть використовуватися, щоб оцінити здатність системи ICT протистояти навмисним спробам обійти системну безпеку. Мета полягає в тому, щоб перевірити систему ICT з точки зору джерела загрози і ідентифікувати потенційні відмови в схемах системні захисту IC. [3].

Перегляд коду є найповнішим (але також і найдорожчим) в дорозі оцінки уразливості [3].

Результати цих типів тестування безпеки допоможуть ідентифікувати уразливості системи [3].

Важливо відмітити, що інструментальні засоби проникнення і методики можуть дати неправдиві результати, якщо не успішно експлуатується уразливість. Щоб експлуатувати специфічну уразливість, треба знати точну систему / додаток / і встановлені виправлення на перевіреній системі. Якщо ці дані не відомі під час тестування, то це не може бути можливим для успішної експлуатації специфічної уразливості (наприклад, отримуючи remote reverse shell12); проте, це все ж можливо, щоб зруйнувати або перезапустити процес, що перевіряється або систему. У такому разі перевірений об'єкт треба також вважати уразливим. Методи можуть включати наступні дії [3]:

- інтерв'ювання у людей і користувачів;

- анкетні опитування;

- фізичне обстеження;

- аналіз документу.

**1.6. Оцінка інформаційних ризиків**

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз і вразливостей, в тому числі комп'ютерного шахрайства, шпигунству, саботажу, вандалізму, пожежі або повені. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз безпеці інформації та ймовірності реалізації загрози [8].

Процес оцінки ризику оцінює ймовірність і потенційний збиток від виявлених загроз, заходи індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності. Потім вимірюється ефективність існуючих заходів. Результати допомагають організації визначити, які активи є найбільш критичними, служать основою для визначення пріоритетів і рекомендують курс дій для захисту активів [8].

Оцінка вважається досягнутою якщо використовуються рекомендації за оцінкою інформації, які покривають такі проблеми як [3]:

- персональна безпека;

- персональна інформація;

- юридичні і регулюючі зобов'язання;

- приведення законів в життя;

- реклама і економічні інтереси;

- дії фінансових втрат/руйнувань;

- громадський порядок;

- політика бізнесу і експлуатації;

- втрата доброзичливості;

- контракт або угода з клієнтом.

Значення активу, загрози і рівня уразливості, наслідки, що відносяться до кожного типу, погоджені в матриці, ідентифікуючи для кожної комбінації відповідну міру ризику в масштабі від 0 до 8. Значення поміщені в матрицю структурним способом (рис. 1.4) [9].

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Ймовірність виникнення загрози | Низька (Н) | | | Середня (С) | | | Висока (В) | | |
| Послаблення в експлуатації | Н | С | В | Н | С | В | Н | С | В |
| Значення активу | 0 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| 3 | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| 4 | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

Рис. 1.4. Приклад міри ризику в масштабі від 0 до 8.

Надамо методику оцінки ризиків для активів організації.

Для кожного активу розглядають відповідну уразливість і їх відповідну загрозу. Якщо є уразливість без відповідної загрози або загрози без відповідної уразливості, то немає тепер ніякого ризику (але треба передбачити, що ця ситуація змінюється). Тепер відповідний рядок в матриці ідентифікований значенням активу, і відповідний стовпець ідентифікований вірогідністю появи загрози і вірогідністю експлуатації. Наприклад, якщо у активу є значення 3, загроза"висока" і уразливість "низька", міра ризику 5. Припустіть, що у активу є значення 2, наприклад, для модифікації, рівень загрози "низьких" і вірогідність експлуатації "висока", тоді міра ризику 4. Розмір матриці, в термінах числа категорій вірогідності загрози, вірогідність категорій експлуатації і числа категорій оцінки активу може бути відкоригована до потреб організації. Додаткові стовпці і рядки вимагають додаткових заходів по ризику. Значення цього підходу знаходиться в ранжируванні ризиків, які використовуватимуться [3,9].

Подібна Матриця (табл.1.8.) виходить з розгляду вірогідності інцидентного сценарію, який відображений проти передбачуваної дії на бізнес. Вірогідність інцидентного сценарію дана загрозою, що експлуатує уразливість з визначеною вірогідністю. Таблиця відображає цю вірогідність проти дії на бізнес, пов'язаної з інцидентним сценарієм. Ризик, що виходить, виміряний в масштабі від 0 до 8, який може бути оцінений проти визначених критеріїв ризику. Цей масштаб ризику міг також бути відображений в простій оцінці абсолютного ризику, наприклад як [10]:

- Низький ризик: 0-2

- Середній ризик: 3-5

- Високий ризик: 6-8

Матриця або таблиця (табл. 1.9) можуть використовуватися, щоб зв'язати коефіцієнти наслідків (значення активу) і вірогідність здійснення загрози (уразливості, що бере до уваги аспекти) [11,3].

Таблиця 1.8 [3].

Таблиця ймовірності проти дії впливу пов’язаного з інцидентним сценарієм

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Ймовірність інцидентного сценарію | Дуже низька | Низька | Середня | Висока | Дуже висока |
| Вплив | Дуже низько | 0 | 1 | 2 | 3  4  5 | 4  5 |
| Низько | 1 | 2 | 3 |
| Середнє | 2 | 3 | 4 | 6  7 |
| Високо | 3 | 4 | 5 | 6 |
| Дуже високо | 4 | 5 | 6 | 7 | 8 |

Перший крок повинен оцінити наслідки (значення активу) в визначеному масштабі, наприклад 1 - 5, кожного активу, якому погрожують (стовпець ―b в таблиці 1.9) [11,3].

Таблиця 1.9.

Зв'язок коефіцієнту наслідків з вірогідністю здійснення загрози

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дескриптор небезпек | Наслідки  (активи)  Цінність (b) | Ймовірність розповсюдження загроз (c) | Міра ризику (d) | Ранжирування небезпеки (e) |
| Загроза A | 5 | 2 | 10 | 2 |
| Загроза B | 2 | 4 | 8 | 3 |
| Загроза C | 3 | 5 | 15 | 1 |
| Загроза D | 1 | 3 | 3 | 5 |
| Загроза E | 4 | 1 | 4 | 4 |
| Загроза F | 2 | 4 | 8 | 3 |

Другий крок повинен оцінити вірогідність входження загрози в визначеному масштабі, наприклад 1 - 5, кожної загрози (стовпець ―c в таблиці 1.9).

Третій крок повинен вичислити міру ризику, множенням (b x c). Нарешті загрози можуть бути ранжирувані в порядку що пов'язаний з мірою ризику. Треба відмітити, що в даному прикладі, 1 узята як найнижчий наслідок і найнижча вірогідність здійсненням загрози [11,3].

**1.7. Висновки по розділу.**

В розділі було надано аналіз та визначення області застосування і межі процесів менеджменту ризиків. Це дозволить створити ефективне функціонування системи менеджменту інформаційної безпеки. Для здійснення комплексу дій, спрямованих на управління СМІБ шляхом уніфікації було надано список обмежень, що зачіпають організацію і визначають орієнтацію її ІБ.

Згідно з темою роботи було ретельно проаналізовано ідентифікацію та оцінку цінності активів. Розглянуто два види активів, надано їх зміст та області застосування. В кінцевому аналізі було визначено, оцінені або призначені значення на актив для визначення ресурсів, які будуть витрачені для захисту активу.

Для оцінки можливих наслідків було визначено критерії оцінки за їх класифікацією.

Інцидент ІБ може впливати на більш ніж один актив, тому на основі системного аналізу було надано визначення впливу та наведені його типи.

Щоб зменшити інциденти впливу було розглянуто технічні методи оцінки вразливості серед яких випробувальний метод, метод перегляду коду, розглядається в атестаційній роботі.

Оцінка ризиків є важливою частиною будь-якого процесу ІБ. ЇЇ використовують для визначення масштабу загроз безпеки інформації та ймовірності реалізації загрози. Процес оцінки ризику оцінює ймовірність і потенційний збиток від виявлених загроз, заходи індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності. Потім вимірюється ефективність існуючих заходів. Результати допомагають організації визначити, які активи є найбільш критичними, служать основою для визначення пріоритетів і рекомендують курс дій для захисту активів.

## Розділ 2. Визначення цілей та завдань політики управління інформаційної безпеки

Система управління інформаційною безпекою СУІБ (англ. information security management system, ISMS) — частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

**2.1.Основні складові загроз**

Загрозою вважається дія або подія, яка в змозі порушити безпеку будьякої системи. Основними складовими загроз є [12,13];

1. Цілі – компоненти безпеки, які підлягають атаці .

2. Агенти – люди або організації, які можуть створювати загрозу.

3. Подія – дії, які створюють загрозу.

Розглянемо більш розлого такий компонент загрози безпеки об’єкта, як агенти. Агентами загроз є люди, які свідомо або підсвідомо можуть чи намагаються нанести збиток організації чи структурі. Для цього вони повинні мати наступне [13,14]:

- Доступ.

- Знання.

- Мотивацію

Первинним компонентом виникнення загроз є мотивація агента для здійснення певних дій. Мотивація є спонукаючою дією, її можна визначити як первісну ціль. В даному випадку мотивацію для досягнення загрози безпеки об’єкта слід розглядати як деструктивний фактор для підприємства чи іншої структури, чия безпека потенційно може бути порушена. Як правило, деструктивною мотивацією є незадоволеність потреб агента щодо його матеріальних або моральних цінностей, тобто можна сказати, що основною причиною виникнення агента загрози є недостатній рівень вмотивованості такого працівника щодо збереження своєї посади і тих благ, які вона несе, а отже і не має достатнього рівня мотивації щодо збереження безпеки підприємства на якому такий агент прац. Відобразимо у вигляді функції рівень вмотивованості агентів загроз РВА [13,14]:

|  |  |
| --- | --- |
| РВА *= f (ІП; НРП;СПР; КІС;ОБП; ВП;СФ)* [14] | (2.1.) [14] |

де *ІП* – імідж посади;

*НРП* – наявність ресурсів, що знаходяться у підпорядкуванні;

*СПР* – рівень самостійності в прийнятті рішень;

*КІС* – рівень комунікативної діяльності в різних ієрархічних структурах управління;

*ОБП* – офіційні бонуси посади;

*ВП* – винагорода за працю;

*СФ* – специфічні об’єктивні фактори для різних країн.

На кожен вище визначений фактор першого порядку, який впливає на рівень вмотивованості агента та задоволення своєю посадою, в свою чергу, діють фактори другого та третього порядку.

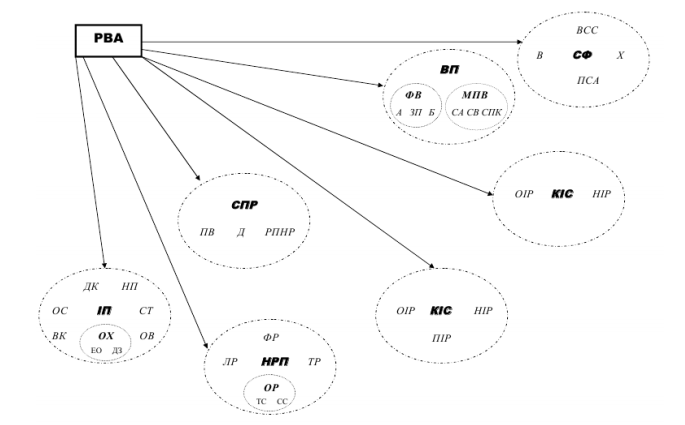


Рис. 2.1. Узагальнена модель управління мотивацією агента загрози

Розглянемо більш детально функціональні області, в межах яких діють фактори першого порядку [13].

1. Будь-який агент на підприємстві чи в організації займає певну посаду, імідж якої залежить від багатьох факторів, а отже є відкритим для багатьох вразливостей, які виникають при цьому. В формулі (2) описано найбільш поширені вразливості, які можуть призвести до виникнення загрози загальної безпеки об’єкта (на мікрорівні – підприємства, організації, фірми і т. п., на макрорівні – області, регіону, країни тощо) шляхом виникнення демотивації агента.

|  |  |
| --- | --- |
| ІП *= f (ОС; ВК; ДК; НП; ОХ; СТ; ОВ)*, [14] | (2.2) [14] |

де *ОС* – особистий секретар (помічник);

*ВК* – власний кабінет;

*Д*К – дизайн кабінету;

*Н*П – назва посади;

*СТ* – марка службово транспорту;

*ОВ* – особистий водій;

*ОХ* – особиста охорона, яка, в свою чергу, залежить від таких факторів третього порядку:

|  |  |
| --- | --- |
| ОХ *= f (ЕО; ДЗ),* [14] | (2.3) [14] |

де *ЕО* – ескорт для охорони;

*ДЗ* – дозвіл на носіння та користування вогнепальної зброї.

2. Формула (4) описує найбільш поширені вразливості різних рівнів, які можуть виникнути через доступ агента до ресурсів, на які знаходяться у його безпосередньому підпорядкуванні.

|  |  |
| --- | --- |
| НРП = *f (ОР; ЛР; ФР; ТР),* [14] | (2.4) [14] |

де *ЛР* – людські ресурси;

*ФР* – фінансові ресурси;

*ТР* – технічні ресурси;

*ОР* – організаційні ресурси, у кількісному вираженні, які, в свою чергу, залежить від таких факторів третього порядку:

|  |  |
| --- | --- |
| ОР = *f (ТС ; СС)* [14] | (2.5) [14] |

де *ТС* – типові структури: бухгалтерія, кадри, різні відділи і т.д.

*СС* – спеціалізовані структури: аналітики, референти, іміджмейкери, секретаріат, перекладачі тощо.

3. Рівень самостійності в прийнятті рішень є фактором, який найбільш чинить вплив на РВА саме на макрорівні, наприклад, якщо агент займає посаду депутата чи міністра країни. Для даного фактору достатньо важко виділити об’єктивні показники другого рівня, які теоретично мають найбільший вплив на цей показник. В формулі (2.6) подано основні з них:

|  |  |
| --- | --- |
| СПР *= f (ПВ; Д; РПНР)* [14] | (2.6)[14] |

де *ПВ* – можливість підвищення кваліфікації, інтерактивне навчання;

*Д* – можливість отримання досвіду (тренінги, відрядження, стимулятори, використання СППР тощо);

*РПНР* – ризик прийняття невірного рішення (розраховується на основі попередньо прийнятих рішень).

Для СПР фактори другого порядку є найбільш тісно взаємопов’язаними та послідовними, такими, що не є взаємо компенсованими. Якщо агент не має можливості постійно підвищувати свою кваліфікацію, не має нових сучасних знань, то він автоматично не має можливості набуття досвіду, що призводить до збільшення ризику прийняття невірного рішення, що, в свою чергу, призводить до зниження рівня самостійності в прийнятті рішень і до де мотивації агента.

4. Будь-який агент на підприємстві чи в організації комунікує з іншими агентами і займає певний ієрархічний рівень у структурі управління, який залежить від багатьох факторів, а отже є відкритим для вразливостей, які виникають при цьому. В формулі (2.7) описано найбільш поширені з них:

|  |  |
| --- | --- |
| КІС = *f (ОІР; НІР; ПІР)* [14] | (2.7) [14] |

де *ОІР* – офіційний ієрархічний рівень агента у внутрішній структурі управління об’єктом (підприємством, організацією, регіоном, країною тощо); *НІР* – неформальний ієрархічний рівень агента у внутрішній структурі управління об’єктом;

*ПІР* – персональний ієрархічний рівень агента у зовнішній комунікативній системі «об’єкт-партнери».

5. Ще одним фактором, який чинить вплив на РВА саме є офіційні бонуси посади агента:

|  |  |
| --- | --- |
| ОБП = *f (ЛІА; ПОБ)* [14] | (2.8)[14] |

де *ЛІА* – лобіювання інтересів інших внутрішніх чи зовнішніх агентів;

*ПОБ* – перспективи отримання офіційних благ після залишення даної посади.

6. Формула (2.9) описує найбільш поширені вразливості різних рівнів, які можуть виникнути через незадоволення агентом винагородою за свою працю:

|  |  |
| --- | --- |
| ВП = *f (ФВ; МПВ)* [14] | (2.9)[14] |

де *ФВ* – фінансова винагорода;

*МПВ* – морально-психологічна винагорода Дані фактори, в свою чергу складаються із таких факторів третього рівня:

|  |  |
| --- | --- |
| ФВ = *f (А; ЗП; Б)* ) [14] | (2.10)[14] |

де *А* – акції;

*ЗП* – основна заробітна плата;

*Б* – різноманітні бонуси у вигляді премій, доплат, надбавок тощо.

|  |  |
| --- | --- |
| МПВ = *f (СА; СВ; СПК)* [14] | (2.11)[14] |

де *СА* – самоактулізація;

*СВ* – самовираження;

*СПК* – соціально-психологічна комфортність [15].

7. Розглянемо специфічні об’єктивні фактори для різних країн на прикладі України. Фактори другого порядку, які подані в формулі (2.12) є найбільш розповсюдженими на території України і особливої загрози набувають на макрорівні На мікрорівні вони, як правило, є найбільш розповсюдженими в організаціях та службах державної форми власності.

|  |  |
| --- | --- |
| СФ = *f (В; Х; ВСС; ПСА)* [14] | (2.12)[14] |

де *В* – можливість «відкатів»;

*Х* – можливість отримання хабарів;

*ВСС* – використання службового становища в особистих цілях;

*ПСА* – надання послуг стороннім взаємопов’язаним організаціям.

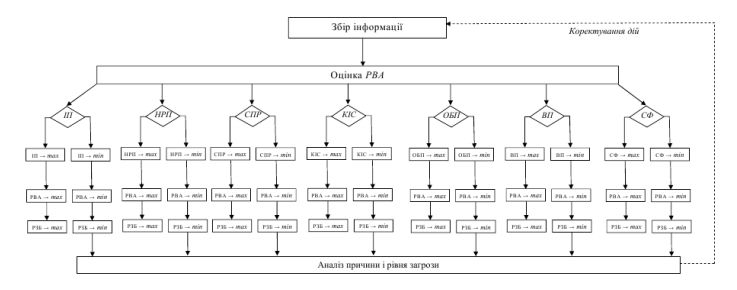


Рис. 2.2. Узагальнений функціональна схема методу оцінки рівня вмотивованості агентів загроз

Метод оцінки рівня вмотивованості агентів безпеки, представлений на рис. 2.2 у вигляді узагальненої функціональної схеми дій, дає можливість, крім оцінювання РВА, також оцінити рівень забезпечення безпеки (РЗБ) на аналізованому об’єкті та завчасно попередити виникнення можливих вразливостей та загроз шляхом коригуючи дій.

**2.2. Потенційні загроиз для інформації в ІС**

Основою для проведення аналізу ризиків і формування вимог до захисту інформації є розробка моделі загроз для інформації та моделі порушника.

**2.2.1. Моделі загроз**

Діяльність всіх осіб, що мають доступ до охоронюваним законом масивів особистої інформації, повинна спиратися на норми, введені «Моделлю». Модель бачить такі види об’єктів кібератак, категорії жертв та методи кібератак (рис. 2.3.) [16].

Їх кроки, які посягають на збереження і цілісність захищених масивів відомостей, можуть принести шкоду інтересам особистості, суспільства, держави [16].

ДССЗІ розробило модель дій цих типів суб'єктів. Зазіхання, за версією документа, можуть відбуватися наступними шляхами [16]:

* перехоплення або знімання інформації, яка направляється по каналах зв'язку, для її копіювання або поширення з будь-якими цілями, такими, що суперечать законодавству [16];
* отримання неправомірного доступу до баз, в яких зберігаються номери паспортів, адреси, медичні історії. Доступ використовується не тільки для копіювання або неправомірного поширення відомостей, а й для їх зміни, знищення, внесення спотворень в важливі параметри. Для деструктивних впливів використовуються спеціальні програмні та технічні засоби, при цьому оператори часто не мають готових відповідей на виклики, створені з використанням сучасних технологій (рис. 2.3) [16].

Розробляючи модель загроз, необхідно пам’ятати, що на її основі кожен конкретний оператор зможе розробити власні методики захисту від загроз власних підприємств. Для цього потрібно правильно використовувати матеріальні засоби зберігання і передачі інформації [16].

Відповідальність за працездатність і захищеність обладнання і мереж несуть їх власники [16].



Рис. 2.3. Складові частини та жертви кібератаки

Завдання, які вирішуються «Моделлю загроз» представлено на рис. 2.4 [16].

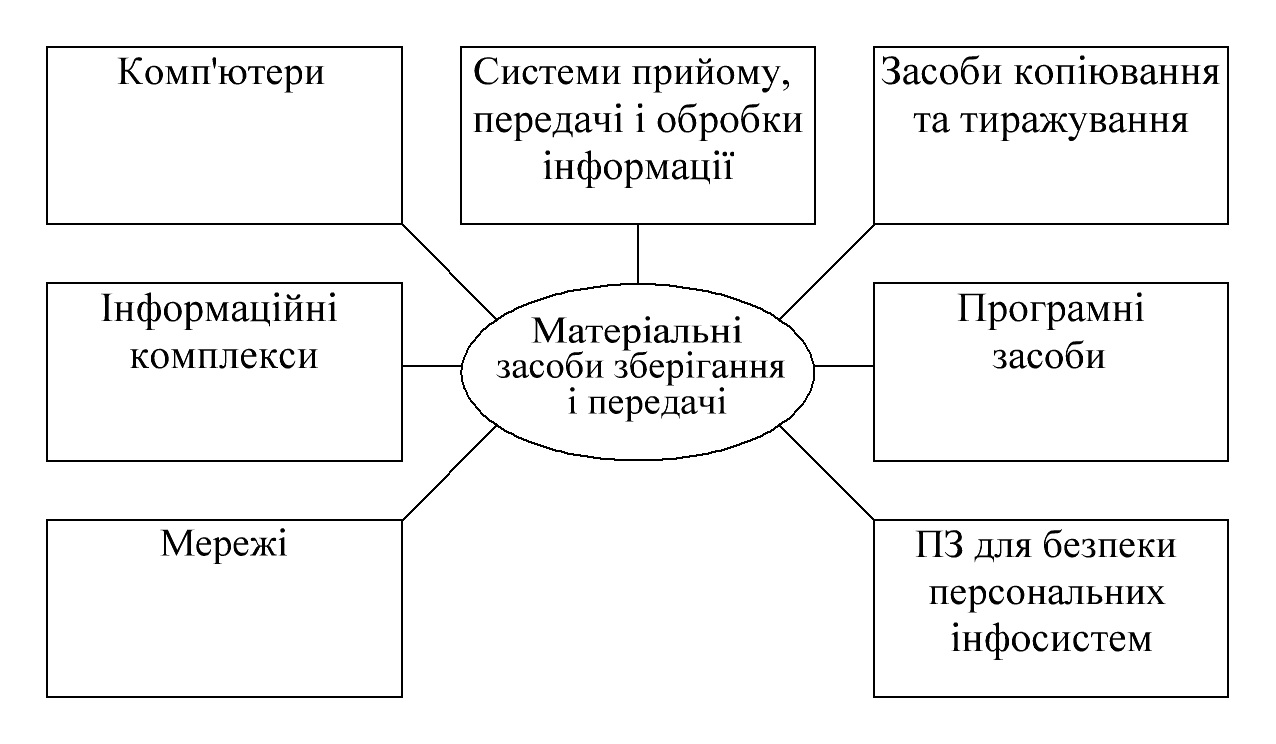


Рис. 2.3. Апаратно-програмні засоби зберігання і обробки інформації.

**2.3. Ризики інформаційних активів.**

Існує серьозна загроза для організацій яка виражається в порушенні основних властивостей інформації. Комп'ютерні шахрайства, шпигунство, саботаж, вандалізм, пожежі або повені ці всі фактори впливають на контроль інформації. Інформаційні ресурси мають якість і кількість, собівартість і ціну, тому оцінка ризиків ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Щоб зменшити потенційні збитки треба визначити масштаб загроз загроз безпеці інформації та ймовірності реалізації загрози.

Спочатку проводять оцінювання ймовірність і потенційний збиток від загроз, їх ставлення до конфіденційності, цілісності та доступності, а потім вимірюється ефективність існуючих заходів. На цьому аналізі визначаються найбільш критичні активи і ця основа служит для визначення пріоритетів і рекомендують курс дій для захисту активів.

Під класичним визначенням «оцінки ризиків» розуміють що це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику [9].

Цей процес включає в себе [9]:

-оцінку ймовірності загроз і вразливостей, які можливі;

-розрахунок впливу, який може мати загроза на кожен актив;

-визначення кількісної (вимірні) або якісної (описуваної) вартості ризику.

Вище зазначенні зміні рідко незалежні одна від одної. Існує зв'язок між вартістю активів впливом та ймовірностю. Другорядний актив має меншу ймовірність компрометації ніж цінний. Необхідно брати до уваги більше ніж просто випадкові дії, а також що при наявності достатнього часу і рішучості, люди мають можливість обійти майже всі заходи безпеки. Мотивація підштовхує людей до творчості. На рисунку 2.1 надана узагальнена модель управління мотивацією агента загрози.

Оцінку інформаційних ризиків можливо проводити трьома способами:

1.методи;

2.управляючі документи;

3.інструменти.

На рисунку 2.4. преставлени способи оцінки інформаційних ризиків.

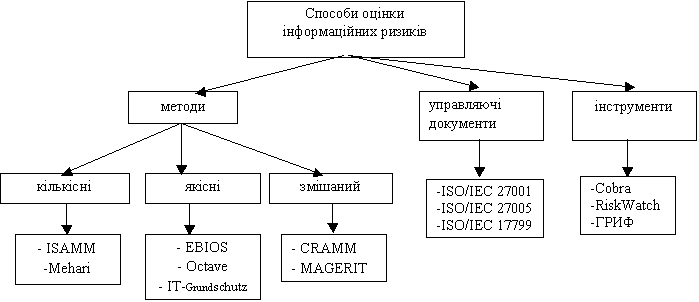


Рис. 2.4. Способи проведення оцінки інформаційних ризиків.

Метод, зазвичай, є покроковою інструкцією з інструментом (програмним продуктом) для проведення оцінки ризиків.

Методи розділяються на такі види –кількісний, якісний або змішаний. Кожен з них має свої переваги та недоліки. Розглянемо їх та визначимо в яких випадках треба їх застосовувати [8,9] .

Кількісні методи. Для визначення вартості активів та імовірності втрати кількісний метод використовує об’єктивні і вимірні дані. Ці дані збираються з метою обчислити числові значення для кожного з компонентів, зібраних в ході оцінки ризиків та аналізу витрат і переваг. Метод поділяється на такі категорії: низький, середній, високий або не важливо, важливо, дуже важливо, або за шкалою (від 1 до 10). Метод має такі переваги і недоліки [8,9].

Переваги [8,9]:

-ризики є приоритетними ніж фінансові налдідки;

-активи є більш приоритетнами ніж фінансові ціності;

-отримання спрощених результатів управління ризиком та поверненням інвестицій у забезпечення безпеки;

-результати можуть бути виражені в управлінській специфічній термінології (наприклад, грошові значення і ймовірність виражається у вигляді певного відсотка);

-точність має тенденцію до збільшення з плином часу, так як організація постійно веде записи даних.

Недоліки [8,9] :

-визначення впливу привласнених ризикам на підставі суб'єктивних думок учасників;

- досягнення надійних результатів потребує консенсусу і займає багато часу;

-розрахунок може бути складним і трудомістким;

-складність представлення результатів в грошовому еквіваленті;

-процес вимагає спеціальних знань, а це потребує складного навчання персоналу.

Якісний метод. В цьому методі використовується відносний показник ризику або вартості активу. Він визначається на основі рейтингу або розподіляється на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10. У якісної моделі оцінка дій та імовірності виявлених ризиків здійснюється швидким та економічно-ефективним спосібом. Набори ризиків які записані та проаналізовані в якісній оцінки ризику можуть бути використані в ціліспрямованій кількісній оцінки [8,9].

Переваги [8,9]:

-забезпечує прозорість і краще розуміння класифікації ризику;

-можливість досягти консенсусу щодо впливу впливу ризику;

-немає необхідності визначати фінансову вартість активів;

-значне легше залучити людей, які не є експертами в області комп'ютерної безпеки.

Недоліки [8,9]:

- відмінність між важливими ризиками недостатня, що дає неадекватне визначення впливу ризику;

-утруднена звітністьпро інвестиції в контроль реалізації, тому що немає підстав для аналізу витрат і переваг;

-необхідність якісної команди управління ризиками для вірних результатів оцінки впливу ризиками.

Змішаний метод. Виходячі з недоліків і переваг якісного і кількісного методу, а головне, що немає великих переваг між ціми методами оцінки ризиків, комбінація кількісного і якісного методу являє собою змішану сукупність переваг і недоліків вище згаданих методів [8,9].

**2.4. Системи управління інформаційної безпеки.**

Система управління інформаційною безпеки базується на аналізі аналізі ризиків є частиною загальної системи управління і призначена для реалізації, проектування, супроводження, контролю та вдосконалення заходів у галузі ІБ. Організаційна структура, дії з планування, політика, процедури, обов’язки, ресурси і процеси.

Захист бізнесу та знань компанії від витоку інформації або знищення її, гарантія майнових прав та інтересів клієнтів є основними призначеннями СУІБ, але вони не повинні обмежувати або ускладнювати процеси обміну інформацією бо це буде заважати розвитку компанії.

СУІБ створюється для забезпечення униможливості несанкціонованого доступу до інформації, що є критичною, збереження конфіденційності важливої інформації, а також цілісності інформації для правильності процесів які пов’язані з цим і ряду інших цілей.

Вище зазначені цілі можуть бути досягненими у ході вирішення таких основних завдань [17]:

-визначення відповідальних за інформаційну безпеку;

-, розробка спектра ризиків інформаційної безпеки;

- проведення їх експертних оцінок;

- розробка політик і правил доступу до інформаційних ресурсів;

- розробка системи управління ризиками інформаційної безпеки;

- методи оцінки ризиків;

-контроль ІБ на підприємстві.

При побудові СУІБ треба чітко визначити взаємопов’язаність процесів та підсистем ІБ, відповідальних за них, трудові та фінансові ресурси для ефективної її роботи, тощо.

Основні функції чкі повинна виконувати СУІБ [17]:

-виявлення та аналіз ризиків інформаційної безпеки;

-планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

-контроль цих процесів;

-внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Принципи, які повинні виконуватися для успішної роботи СУІБ наступні [17]:

-комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі підприємства та за її межами;

-узгодженість з бізнес-задачами і стратегією підприємства;

-високий рівень керованості;

-адекватність інформації, яка використовується і генерується;

-ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

-безперервність управління;

-процесний підхід – зв’язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв’язку між етапами.

Успішність роботи системи управління ІБ – це дотримання при її побудові міжнародних стандартів зокрема стандарту ISO/ІЕС 27001, який надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

Остання версія міжнародного стандарта ISO/ІЕС 27001 яка була введена датована 20013 роком.

В новій редакції введена нова вимога щодо необхідності чіткого переліка осіб як внутрішніх так і зовнішніх з якими необхідно взаємодіяти при вирішенні питань з керування інформаційної безпеки. При визначенні інформації яка повина бути доведена до осіб що мають зацікавленість в неї, компанія визначитись коли й хто повинен це зробити [18]. Це нововведення на думку розробників стандарту спрощує залучення до керуванням ІБ керівництва та власників бізнес-процесів тому що тепер когут отримати всю актуальну інформацію по функціонуванню та управлінням ІБ.

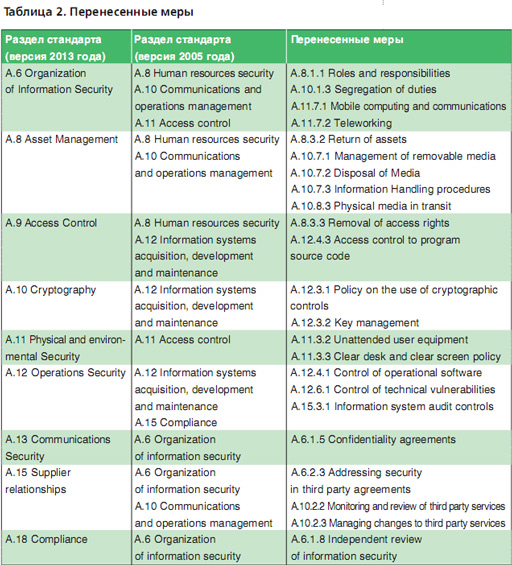
Редакція 2013 року цього стандарту вводить єдина вимога до любої документованой інформації [18].

В новой редакції враховано відсутність чіткої структури вимог до формуліровки завдань та планування їх виконання (це було рознесено по різним розділам стандарту), тому тепер все поєднано в розділі «Мониторінг, зміни, аналіз та оцінка» [18].

Нова версія містить 113 мір забезпечення інформаційної безпеки на відміну від попередній яка містила 133 міри. Хоч більшість мір не змінилась, але в новій редакції збільшилось кількість розділов додатку з 11 до 14. Всього було перенесено 23 міри (табл. 2.1) [18].

Таблиця 2.1.

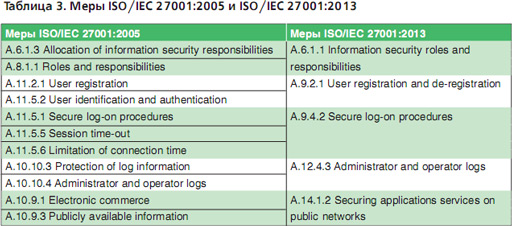
Перенесені міри



В нової редакції було логічно поєднано деякі міри (в кількісті 5), наприклад міри «Електронна комерція» і «Загальнодоступна інформація поєднанні в міру «Захист сервісів серверів додатків в публічних мережах» (табл. 2.2) [18].

Таблиця 2.2.

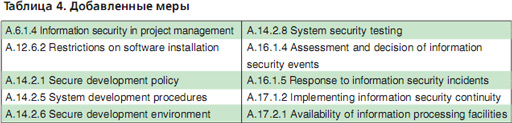
Міри ISO/ІЕС 27001:2005 і ISO/ІЕС 27001:2013



Для забезпечення інформаційної безпеки було добавлено 10 нових мір. Докладні інструкції по їх використанню наведені в оновленому стандарті ISO/ІЕС 27002:2013 (табл. 2.3) [19].

Таблиця 2.3.

Добавлені міри



26 мір було признано неактуальними, або такі що дублюють вимомоги оновленого стандарту, або такі що інші міри включають їх до себе.

**2.6. Висновки по розділу.**

В розділі 2 було розглянуто розлого такий компонент загрози безпеки об’єкта, як агенти. Агентами загроз є люди, які свідомо або підсвідомо можуть чи намагаються нанести збиток організації чи структурі, тобто мають мотивацію. На основі первиних компонентов виникнення загроз було надано узагальнена схема причин мотивації агента загроз.

Розглянуто класифікацію загроз, спосіби їх атак та надано об’єкти що піддаються нападам. На основі моделей загроз було надані впливи на інформаційні активи за оцінками ризиків й імовірності їх впливів.

Виходячі з того що система управління інформаційної безпеки гарантує захист бізнесу та знань компанії від витоку інформації або знищення її, майнові права та інтереси клієнтів, а тому потребує постійної модифікації. В розділі було надано останні зміни до міжнародного стандарту що регулює методи виконання завдань СУІБ.

**Розділ 3. Налаштування та експериментальне дослідження системи.**

**3.1 Призначення і цілі створення системи.**

В даний час одним з ключових напрямків інформаційної безпеки в багатогалузевих компаніях є досягнення максимальної синергії та консолідації в СМІБ.

Внаслідок інтеграції в Систему максимальної кількості необхідних для управління інформаційної безпекою даних, буде сформована єдина інформаційна інфраструктура в СМІБ, що дозволяє удосконалювати інформаційну проникність і синергію між структурними підрозділами.

**3.1.1 Призначення Системи**

Спеціалізована експертна Система «Портал ESS» призначена для здійснення комплексу дій, спрямованих на управління системою менеджменту Інформаційної безпеки шляхом уніфікації і підвищення ефективності процесів ІБ в вертикально-інтегрованих багатогалузевих компаніях.

Програма містить в собі такі пов'язані між собою модулі:

• модуль інвентаризації інформаційних активів;

• реєстр ризиків і вразливостей;

• реєстр інцидентів;

• щоденник менеджера ІБ;

• досьє співробітників підприємства;

• основні типові документи, що регламентують роботу СМІБ;

• модуль звітів, що настроюються і статистики;

• модуль допомоги (дерево реагування, мануали, актуальні питання і т.д.).

Система повинна забезпечувати єдину інформаційну інфраструктуру в СМІБ, створювану через інтеграцію максимальної кількості інформації в модулі і, тим самим, що дозволяє удосконалювати інформаційну проникність і синергію між структурними підрозділами.

За класифікацією автоматизованих комплексів Система відноситься до багатофункціональних програмно-технічних комплексів для автоматизації управління організаційними процесами в умовах розподіленого використання інформації різними фахівцями.

**3.1.2 Цілі створення Системи**

Відповідно до концепції створення та розвитку Системи до стратегічних цілей можна віднести:

• вдосконалення процесу управління СМІБ в вертикально-інтегрованих багатогалузевих компаніях;

• підвищення інформаційної підтримки структурних підрозділів;

• підвищення ступеня прозорості інформаційної взаємодії між структурними підрозділами в області СМІБ;

• виконання стандарт утворює ролі для всіх елементів СМІБ;

• формування єдиної інформаційної інфраструктури в області СМІБ;

• зниження тимчасових витрат на інформаційне забезпечення процесів СМІБ;

• підвищення ефективності захисту інформаційних активів на основі інтеграції їх в єдиний інформаційний простір і оперативності доступу до інформаційних активів, ризиків і інцидентів всім зацікавленим особам;

• координація та стимулювання проведення заходів щодо вдосконалення СМІБ;

• забезпечення максимального доступу до інформації про підтримку в області СМІБ на всіх рівнях;

• забезпечення оперативного інформаційного взаємодії потенційних користувачів Системи між собою на основі організації «єдиної точки входу», за допомогою публікацій, інтерфейсів обміну даними та інших сервісів Системи.

Досягнення перелічених цілей повинно привести до наступних позитивних результатів:

• підвищення прозорості діяльності (формування системи online-моніторингу);

• підвищення ефективності роботи СМІБ;

• додаткового економічного ефекту в області СМІБ;

• забезпечення системи зворотного зв'язку (інформація «з перших рук») та інформаційної підтримки в області СМІБ, в результаті - підвищення ефективності роботи СМІБ.

**3.2.1 Вимоги до Системи в цілому**

Спільними для Системи в цілому є наступні вимоги:

• Система повинна містити необхідний обсяг інформації, механізм своєчасної актуалізації змісту і базовий набір сервісів роботи з інформацією, що забезпечує необхідну повноту інформаційних та інших сервісів, що надаються користувачеві;

• структура подання інформаційних активів і призначені для користувача інтерфейси з доступу до активів і сервісів повинні бути інтуїтивно зрозумілі користувачам;

• надані послуги повинні мати очевидну цінність для користувачів Системи;

• призначений для користувача інтерфейс повинен забезпечувати вибір типового профілю відповідно до прав користувачів.

При розробці Системи повинні передбачатися:

• розробка, оцінка та вибір моделі побудови інфраструктури Системи з урахуванням інформаційних, технологічних, організаційних та фінансових аспектів, а також заходів щодо забезпечення необхідного рівня інформаційної безпеки;

• розробка стандартів представлення даних і опису інформації в складі Системи;

• розробка стандартних процедур інформаційної взаємодії при управлінні інфраструктурою і інформаційним наповненням Системи;

• забезпечення взаємодії адміністраторів і користувачів при наповненні і супроводі інформаційних активів Системи;

• розробка методів моніторингу стану, використання і періодичності оновлень даних і сервісів Системи.

В Системі має бути враховано наступне:

• перспектива інтеграції Системи в інформаційну систему будь-якого зацікавленого підприємства;

• рівень готовності потенційних користувачів до використання Системи і можливості вдосконалення загальної і професійної культури інформаційної взаємодії;

• необхідність забезпечення гнучкості та оперативності в налаштуванні і модернізації інфраструктури Системи як на рівні адміністрування, так і на рівні проектної модернізації;

• реальні і перспективні потреби потенційних користувачів в інформаційних ресурсах і сервісах Системи;

• необхідність включення в інфраструктуру Системи механізмів підтримки постійного діалогу та взаємодії між користувачами Системи з актуальних тем і питань.

Основними принципами створення Системи є:

• використання будь-якого програмного і апаратного забезпечення, здатного працювати з мережею Інтернет;

• використання загальновизнаних і широко використовуваних стандартів структурування інформації та опису сервісів;

• відповідність міжнародним стандартам у сфері ІБ;

• уніфікація форматів і протоколів інформаційного обміну;

• використання ефективних методів захисту від несанкціонованого доступу до інформаційних ресурсів.

**3.2.2 Вимоги до структури доступу в Систему.**

В Системі повинні бути передбачені три основні категорії користувачів:

• авторизований користувач. Має повний доступ до інформації та сервісів Системи в обсягах фронт-офісу в своєму підрозділі;

• адміністратор. Має повноваження для затвердження інформації, яка підлягає публікації в своєму підрозділі. Права адміністратора можуть бути обмежені певними розділами Системи. Для того, щоб деяка публікація стала доступною в Системі, необхідно отримати твердження інформаційного матеріалу супер-адміністратором;

• супер-адміністратор (контент адміністратор, оператор форм, експерт, модератор). Авторизований користувач, що володіє повноваженнями для створення нових і редагування існуючих інформаційних матеріалів Системи., А також володіє повноваженнями з управління користувачами і адміністраторами, і правами доступу користувачів до інформаційних активів Системи, перегляду журналу дій авторизованих користувачів у всіх підрозділах.

Система повинна забезпечувати коректне поділ прав користувачів. Базове програмне забезпечення Системи повинні бути перевіряємі на відсутність відомих вразливостей до атак на відмову і на несанкціонований доступ.

Система повинна бути захищена від несанкціонованого доступу і зміни вмісту порталу стандартними засобами використовується web-сервера і операційної системи.

Вхід кожного користувача в Систему повинен здійснюватися за допомогою парольної аутентифікації. Кожному користувачеві може бути надано право на вчинення певних дій з тими чи іншими типами документів і розділами Системи

Докладний перелік дій в Системі, доступних для різних категорій користувачів, наведено в Таблиці 3.1.

Підсистема зберігання даних повинна забезпечувати зберігання в БД Системи і вибірку з БД об'єктів для формування змісту Системи.

Таблиця 3.1.

Перелік дій Системи

|  |  |  |  |
| --- | --- | --- | --- |
| Дії | Супер-адміністратор | Адміністратор | Користувач |
| Внесення відомостей про інформаційні активах |  |  |  |
| Внесення відомостей про інциденти |  |  |  |
| Внесення відомостей про співробітників |  |  |  |
| Внесення відомостей про ризики і вразливості |  |  |  |
| Видалення інформації з Системи на рівні Підрозділи |  |  |  |
| Видалення інформації з Системи на рівні Групи |  |  |  |
| Узгодження внесення відомостей на рівні Підрозділи |  |  |  |
| Узгодження внесення відомостей на рівні Групи |  |  |  |
| Узгодження видалення інформації з Системи на рівні Підрозділи |  |  |  |
| Узгодження видалення інформації з Системи на рівні Групи |  |  |  |
| Перегляд інформації всіх Підрозділів Групи |  |  |  |
| Перегляд статистики всіх Підрозділів Групи |  |  |  |
| Додавання і видалення облікових записів |  |  |  |
| Завантаження документів і шаблонів |  |  |  |
| Надання прав адміністратора |  |  |  |
| Надання прав користувача |  |  |  |
| Додавання опцій в розгортаються списки |  |  |  |

Підсистема зберігання даних повинна забезпечувати зберігання в БД Системи і вибірку з БД об'єктів для формування змісту Системи.

**3.2.3 Перспективи розвитку, модернізації Системи.**

Повинна бути передбачена можливість додавання нових функцій в Систему, поліпшення коду Системи (ре факторинг коду, що дозволяє виявити похибки в проектуванні і реалізації окремої функції до того, як помилки будуть визначати стиль розробки).

Повинна бути передбачена можливість розширення механізму аутентифікації і персоналізації змісту відповідно до появи нових вимог до Системи.

Повинна бути передбачена можливість вдосконалення механізму публікації, спрощення та зведення до допустимого мінімуму дій з розміщення інформації в Системі.

Справжнє ТЗ описує вимоги до розробки першої (експериментальної) версії Системи.

**3.2.4 Вимоги до надійності.**

Система повинна забезпечувати відновлення інформації при програмно-апаратних збоїв (відключення електроживлення, відмовах носіїв інформації, віруси і т.д.), стабільність роботи в розрахованому на багато користувачів режимі і живучість Системи при виході з ладу окремих її компонентів.

**3.2.5 Вимоги щодо збереження інформації при аваріях.**

Збереження інформації при збоях і аваріях повинна досягатися для баз даних, файлів даних на файлових серверах - за рахунок архітектури побудови технічних засобів і програмного забезпечення Системи.

При цьому, повинно бути забезпечено автоматичне відновлення даних в базах даних і відновлення файлів з даними на серверах за станом на момент часу, що не перевищує більш ніж 10 годин від моменту збою або аварії технічних і програмних засобів, що забезпечують зберігання цих даних.

Крім цього, повинна бути передбачена система довгострокового архівування даних і файлів, розміщених на серверної частини системи, для забезпечення схоронності вищевказаних даних в разі форс-мажорних обставин, пожеж, стихійних лих і т.д. Повний архів даних повинен формуватися з періодичністю, встановленої адміністратором, або по досягненню критичного розміру попереднього архіву (за замовчуванням). Кожен архів повинен формуватися в двох примірниках, один з яких повинен зберігатися безпосередньо в місці розміщення Системи, інший - в приміщенні з контрольованим обмеженим доступом (порядок доступу до архіву повинен визначатися керівництвом служби ІБ) в будівлі, відмінному від того, де фізично розміщена Система.

Для забезпечення схоронності призначених для користувача даних архітектурою побудови Системи повинно бути передбачено зберігання інформації виключно в базах даних і файлах, що розміщуються на серверах Системи.

**3.2.6 Вимоги до ергономіки та технічної естетики.**

Дизайн Системи повинен відповідати таким вимогам по ергономіки та технічної естетики:

• адекватно відображатися в залежності від типу підключення користувача і від його особистих переваг;

• бути достатньо «легким» за обсягом графічних елементів і забезпечувати якомога більшу швидкість завантаження модулів Системи;

• забезпечувати легку ідентифікацію розділу Системи, в якому знаходиться користувач;

• забезпечувати мінімум зусиль і тимчасових витрат користувача для навігації по розділах Системи;

• володіти розвиненою системою пошуку інформації;

• коректно відображатися при всіх можливих дозволах і кількості одночасно відображаються монітора;

• володіти системою контекстних підказок на сторінках, де у користувача потенційно можуть виникнути труднощі;

• забезпечувати прийнятний результат при роздруківці сторінок Системи на принтері;

• коректно відображати інформацію на комп'ютерах без встановлених флеш-модулів, з відключеною підтримкою скриптів і ін .;

• передбачати можливість підтримки мульти мовний змісту;

• передбачати можливість кроссплатформенной підтримки;

передбачати сумісність з популярними браузерами.

**3.2.7 Вимоги до функцій (завдань), що виконуються Системою.**

Інтерфейс Системи повинен забезпечувати наочне, інтуїтивно зрозуміле уявлення структури, розміщеної на ньому інформації, швидкий і логічний перехід до розділів і сторінок. Навігаційні елементи повинні забезпечувати однозначне розуміння користувачем їхнього змісту: посилання на сторінки повинні бути забезпечені заголовками і коментарями (підказками), умовні позначення відповідати загальноприйнятим. Графічні елементи навігації повинні бути забезпечені альтернативної підписом.

Система повинна забезпечувати навігацію по всім доступним користувачеві ресурсів і відображати відповідну інформацію. Для навігації повинна використовуватися система контент-меню, яке має являти собою текстовий блок (список гіперпосилань). Місце розташування меню на сторінці залежить від затвердженого дизайну типовий сторінки. Всі номери нові сторінки і елементи повинні відкриватися в новій вкладці.

**3.2.8 Пошук інформації.**

Для пошуку інформації повинна застосовуватися пошукова система, розроблена для порталу в залежності від типу використовуваних баз даних. Пошук інформації в документах повинен здійснюватися засобами бази даних, використовуваної при розробці.

Крім загального пошуку, повинні бути доступні локальні пошукові інтерфейси і фільтри, призначені для пошуку специфічної інформації в конкретних розділах Системи.

Пошук повинен здійснюватися за принципом максимальної релевантності.

**3.2.9 Наповнення інформацією.**

Сторінки всіх розділів сайту повинні формуватися програмним шляхом на підставі інформації з баз даних на сервері.

Наповнення інформацією повинно проводитися з використанням спеціальних форм введення. Повинна бути передбачена можливість розміщення інформації, посилань і файлів будь-якого формату, розміщення і форматування тексту, графічній, табличній і мультимедійної інформації.

Після здачі Системи в експлуатацію інформаційне наповнення розділів, включаючи обробку та підготовку до публікації графічних матеріалів, має здійснюватися Замовником самостійно.

**3.2.10 Можливість розширення.**

Додавання нових функціональних можливостей не повинно призводити до погіршень в раніше розроблених і експлуатованих частинах Системи. Взаємодія з зовнішніми інформаційними системами, якщо воно буде потрібно, повинно будуватися на використанні загальноприйнятих відкритих стандартів передачі і структурування інформації. Даний документ описує функціонал першої версії Системи, що повинно враховуватися при її розробці.

**3.2.11 Простота впровадження, підтримки і адміністрування**

Регламентні процеси установки на новому комплекті обладнання, підтримки і адміністрування повинні бути описані в документації і детально опрацьовані в ході реалізації Системи з урахуванням забезпечення їх простоти і зручності. При цьому повинні бути явно сформульовані вимоги до кваліфікації персоналу, який буде експлуатувати Систему.

**3.3 Автоматизація модуля інформаційних активів**

Для скорочення часу обробки даних моніторингу в Систему було введено уніфікаційні дані баз інформаційних активів.

**3.3.1 Характеристика об'єкта автоматизації**

В даний час одним з ключових напрямків інформаційної безпеки в багатогалузевих компаніях є досягнення максимальної синергії та консолідації в СМІБ. З огляду на це, логічним кроком стануть удосконалення наступних областях:

• підвищення ефективності роботи служб ІБ в вертикально-інтегрованої багатогалузевий компанії і вибудовування відмовостійкої системи реагування на події ІБ;

• реалізація комплексної системи заходів щодо зменшення загроз ІБ;

• приведення до єдиних стандартів моделей взаємодії між службами ІБ підрозділів Групи, а також більш чіткий поділ їх відповідальності всередині вертикалі СМІБ, вибудовування чіткої системи взаємної підзвітності.

При цьому виділяється ряд основних напрямків, за якими відбувається автоматизація і консолідація процесів СМІБ, серед яких одним з найважливіших є поліпшення якості та ефективності роботи служб ІБ.

З цією метою вводяться єдині стандарти, форми і методи роботи в рамках СМІБ, співробітники служб ІБ отримують можливість оперативного взаємодії та експертної підтримки при максимальній прозорості роботи СМІБ. Саме такий підхід до побудови СМІБ використовується в провідних світових стандартах в області ІБ в даний час.

В даний момент в підрозділах Групи відсутня єдність механізмів роботи, що викликає певну ентропію і низький ступінь консолідації. З огляду на, що інформаційні потреби кожного з підрозділів мають досить високий ступінь спільності, впровадження єдиної системи централізованого управління процесами СМІБ істотно підвищить функціональні можливості використовуваних рішень і дозволить виключити неуніфікованих, витратні процеси підготовки, узгодження, затвердження і реалізації.

Для досягнення єдності механізмів і узгодженості роботи служб ІБ необхідно:

• забезпечення активної участі представників служб ІБ ключових підрозділів Групи в розробці та обговоренні спеціалізованої експертної системи;

• сприяння представників служб ІБ всіх підрозділів Групи в рамках надання інформації, необхідної для побудови максимально релевантної і зручної системи централізованого управління СМІБ;

• забезпечення відкритого доступу всіх відповідальних співробітників служб ІБ до інформації, необхідної в процесі їх діяльності.

**3.3.2 Автоматизація модуля.**

В рамках управління інформаційною безпекою одним з найважливіших процесів є процес обліку і класифікації об'єктів захисту, або так званих інформаційних активів. K інформаційних активів компанії зазвичай відносять інформацію, апаратне, програмне забезпечення та інші засоби, необхідні для отримання, обробки та зберігання даних, які використовуються в певних бізнес-процесах. Це можуть бути сховища даних, бази даних, бази клієнтів, виробничі показники (звіти), фінансові звіти, інформаційні системи і т. ін. Найчастіше процес підтримки даних про інформаційні активах в актуальному стані представляється скрутним, враховуючи складність інформаційної інфраструктури, велика кількість прикладних систем, де обробляється інформація обмеженого доступу, великий перелік критичних активів, які підлягають захисту т. ін. Зазначені особливості обумовлюють необхідність використання засобів автоматизації для підтримки процесів управління ІБ.

**3.3.3 Опис модуля.**

Модуль призначений для автоматизації діяльності співробітників департаменту інформаційної безпеки, а також власників інформаційних активів. Головною метою автоматизації каталогу інформаційних активів є оптимізація та удосконалення системи управління ІБ.

**3.3.4 Опис рішення**.

Рішення реалізовано на базі програмного забезпечення з закритим вихідним кодом і являє собою готовий інструмент для оцінки та обробки ризиків інформаційних активів компанії. Для роботи з системою не потрібна установка додаткових клієнтських додатків, достатня наявність будь-якого сучасного браузера. Рішення включає в себе такі можливості:

- Централізоване зберігання інформації по всіх об'єктах оцінки ризиків;

- Централізоване зберігання інформації за наявними уразливості ІБ, ймовірним загрозам і ризикам, пов'язаним з реалізацією загроз;

- Проведення оцінки ризиків для кожного інформаційного активу відповідно міжнародним стандартам;

- Розробка плану обробки ризиків і призначення завдань виконавцям за його реалізації;

- Розмежування прав доступу користувачів до інформації в системі відповідно до рольової моделі;

- Можливість одночасної роботи користувачів при проведенні оцінки ризиків;

- Відправлення повідомлень власникам інформаційних активів про внесення змін до оцінку;

- Можливість перегляду всіх дій над об'єктами системи;

- Побудова звітів з інформацією про оцінку ризиків, а також плані обробки ризиків з можливістю вивантаження в Excel.

**3.3.5 Завдання, які вирішуються.**

Процес автоматизації спрямований на оптимізацію та удосконалення системи управління ІБ, створення реєстру інформаційних активів і управління записами. Саме в ньому концентруються дані про всі активи компанії, визначається їхня критичність, ступінь впливу на бізнес-процеси компанії і надалі ці дані можуть використовуватися в модулі.

• Формування довідників активів компанії;

• Оцінка критичності об'єктів захисту;

• Класифікація активів і передача їх в модуль;

• Інтеграція з системами інвентаризації;

• Створення єдиного інформаційного середовища для взаємодії з суміжними системами.

**3.4 Етапи та результати виконання проекту.**

Проект автоматизації модуля інформаційних активів проходить через наступні етапи:

1. Інвентаризація інформаційних активів. Визначення всіх інформаційних активів компанії та поточного їх стану.

2. Категоризація інформаційних активів. Визначення ключових активів, від яких залежить функціонування бізнес-процесів компанії.

3. Логічне проектування процесу управління каталогом інформаційних активів. Структурування, опис та проектування процесів для подальшої автоматизації.

4. Автоматизація процесу управління каталогом інформаційних активів.

5. Проектування розроблених процесів на систему автоматизації. Автоматизація процесів.

В результаті автоматизації модуля інформаційних активів формується перелік активів, визначається їхня критичність з урахуванням впливу на бізнес-процеси компанії, а також створюються матриці доступу для розподілу прав до інформаційних активів. Автоматизація модуля інформаційних активів дозволяє:

• Забезпечити оперативну підтримку в актуальному стані інформації про активи в умовах обмеженого штату співробітників і великої кількості облікових об'єктів;

• Забезпечити застосування єдиних ідентифікаторів активів, що дозволяють використовувати дані для реалізації інших процесів управління інформаційною безпекою (управління ризиками, управління інцидентами).

**3.5 Налаштування системи моніторингу ІА.**

**3.5.1 Користувач.**

Для редагування властивостей користувача необхідно в лівому верхньому кутку в меню, яке викликається натисканням на ім'я користувача, вибрати пункт "профіль" (рис. 3.1).

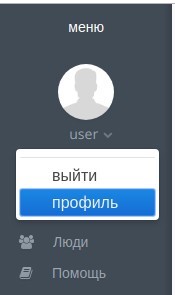


Рис. 3.1. Вибір профілю

Після чого буде відкрито вікно редагування профілю користувача (рис. 3.2).

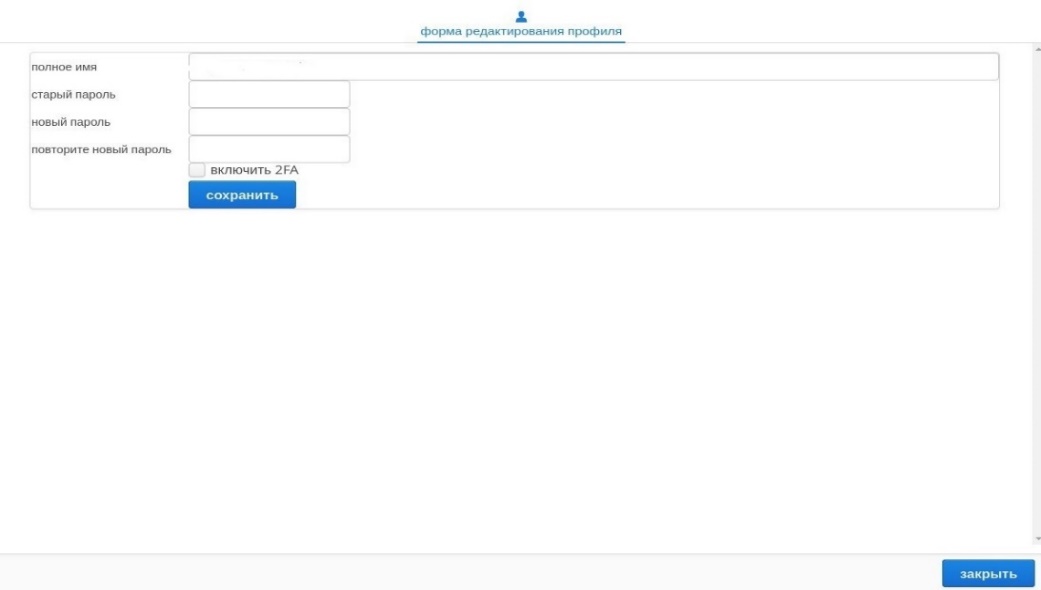


Рис. 3.2. Вікно редагування профілю користувача

**3.5.2 Двухфакторна авторизація**.

Для включення двухфакторной авторизації (далі 2FA) для свого облікового запису необхідно встановити параметр "включити 2FA" (рис. 3.3), після чого в формі з’явиться QR-код, який необхідно сканувати додатком Google Authenticator.

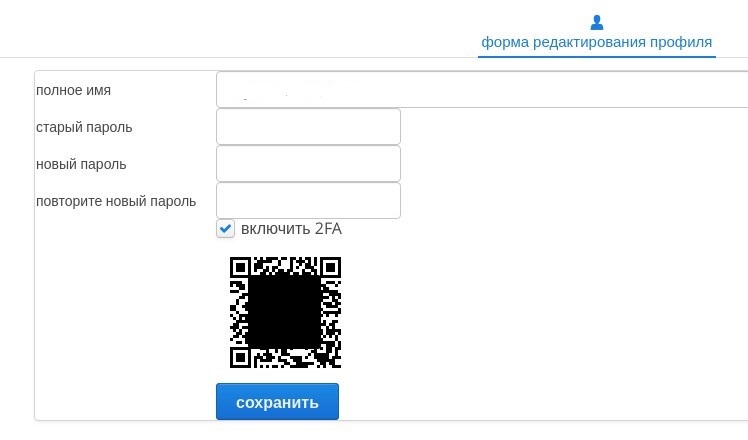


Рис. 3.3. Двуфакторна авторизація

Після успішної активації 2FA форма входу в систему змінить свій вигляд. Після введення логіна і пароля буде відображено додаткове поле OTP, код для якого знаходиться у вас в телефоні в Google Authenticator.

**3.5.3 Головна сторінка.**

На головній сторінці відображені:

- Перелік відкритих вразливостей; (рис. 3.4):

- Список інцидентів;

- Статистика записів в базу даних.

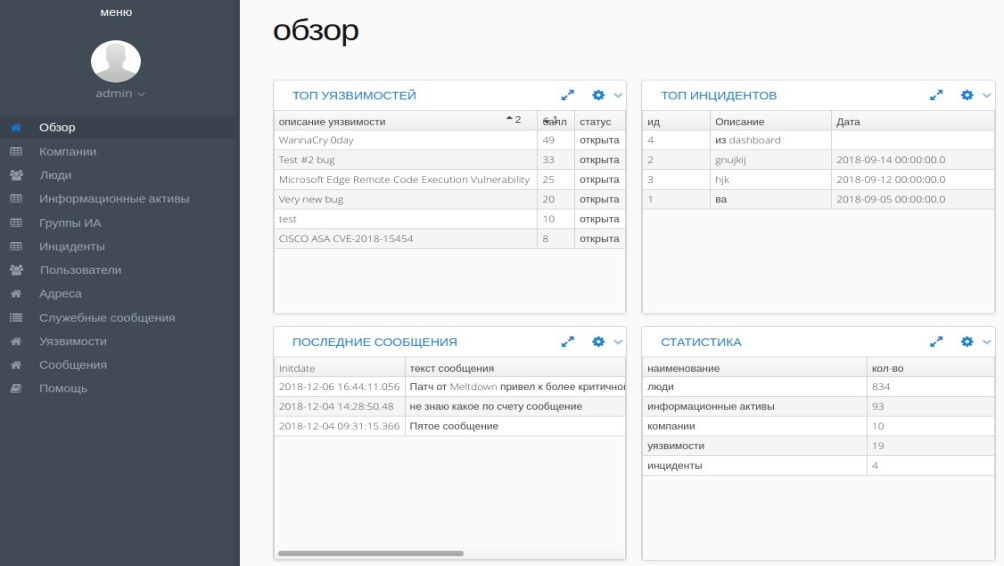


Рис. 3.4. Вікно головної сторінки.

При виборі уразливості в списку її можна відредагувати. Редагується тільки одна уразливість, а не всі із запису (рис. 3.5.).

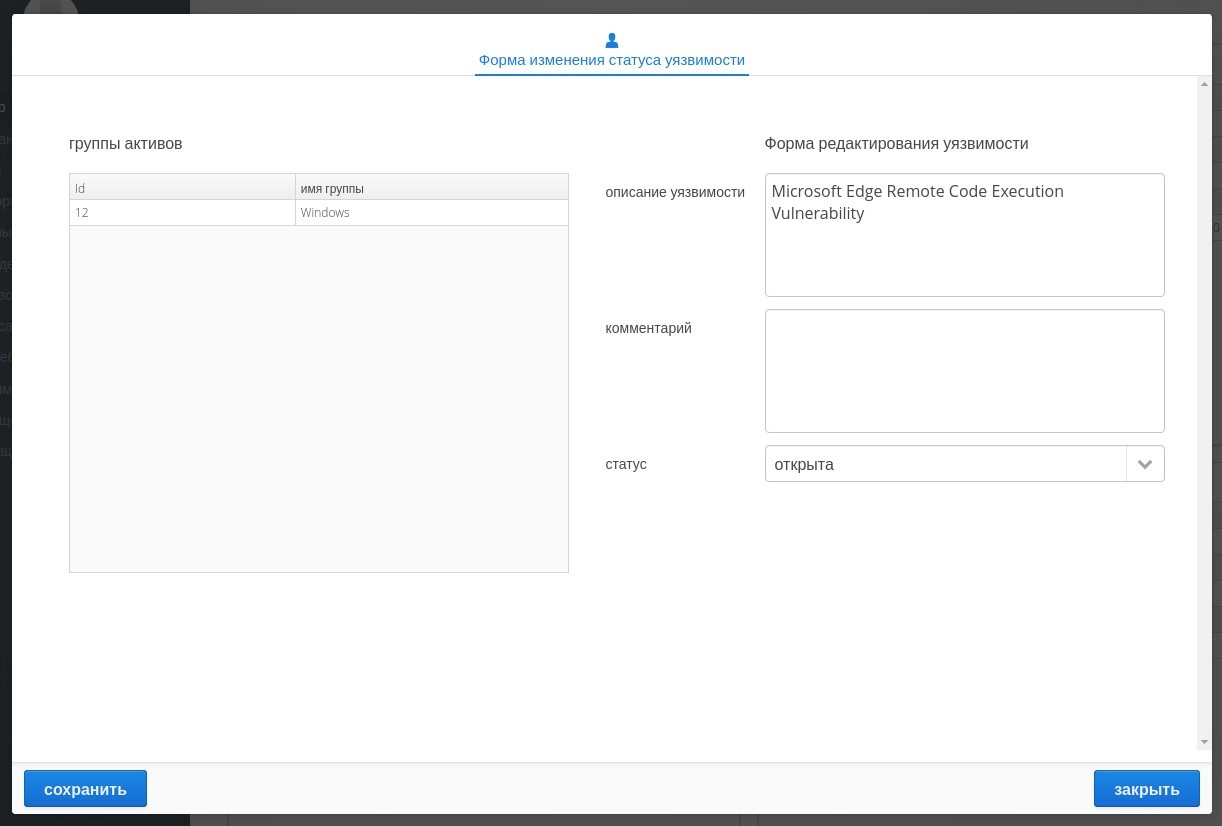


Рис. 3.5. Викно списку вразливостей.

**3.5.4 Вразливості.**

Форма редагування вразливостей представлена на рисунку 3.6.

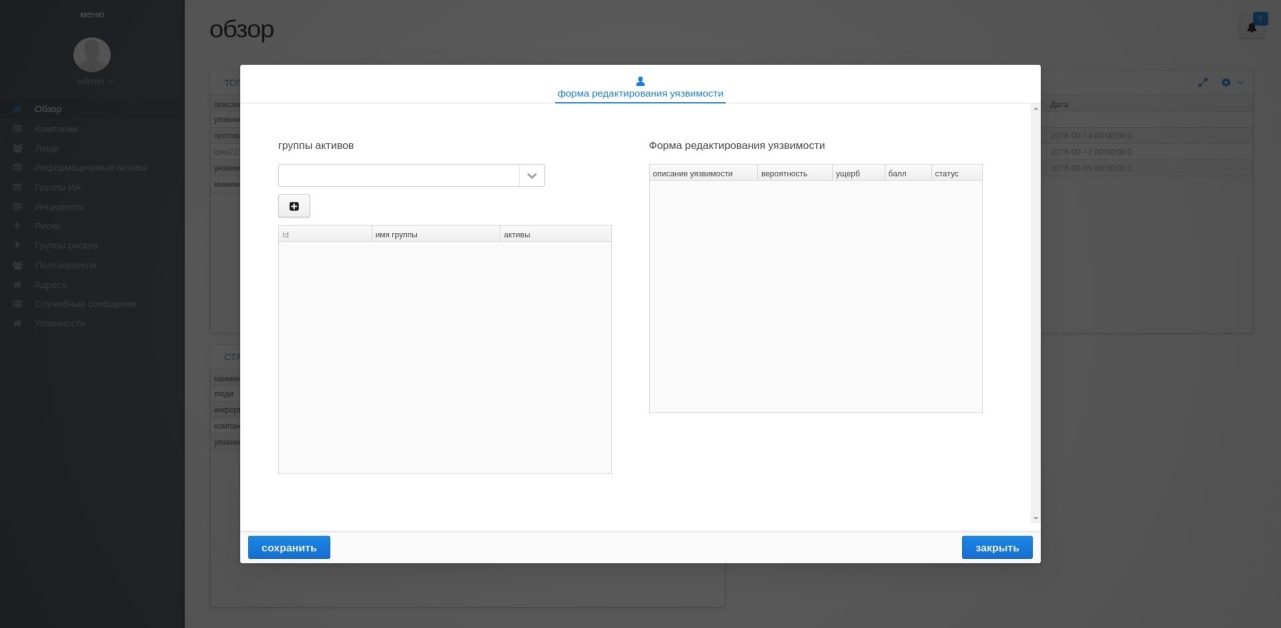


Рис.3.6. Вікно редагування.

**3.5.5 Створення нової групи активів.**

Натиснувши на "+" в попередньому вікні відкриється форма створення нової групи активів, в якій потрібно вказати назву групи і вибрати активи для групи (рис. 3.7). Для збереження необхідно натиснути на кнопку "Зберегти".

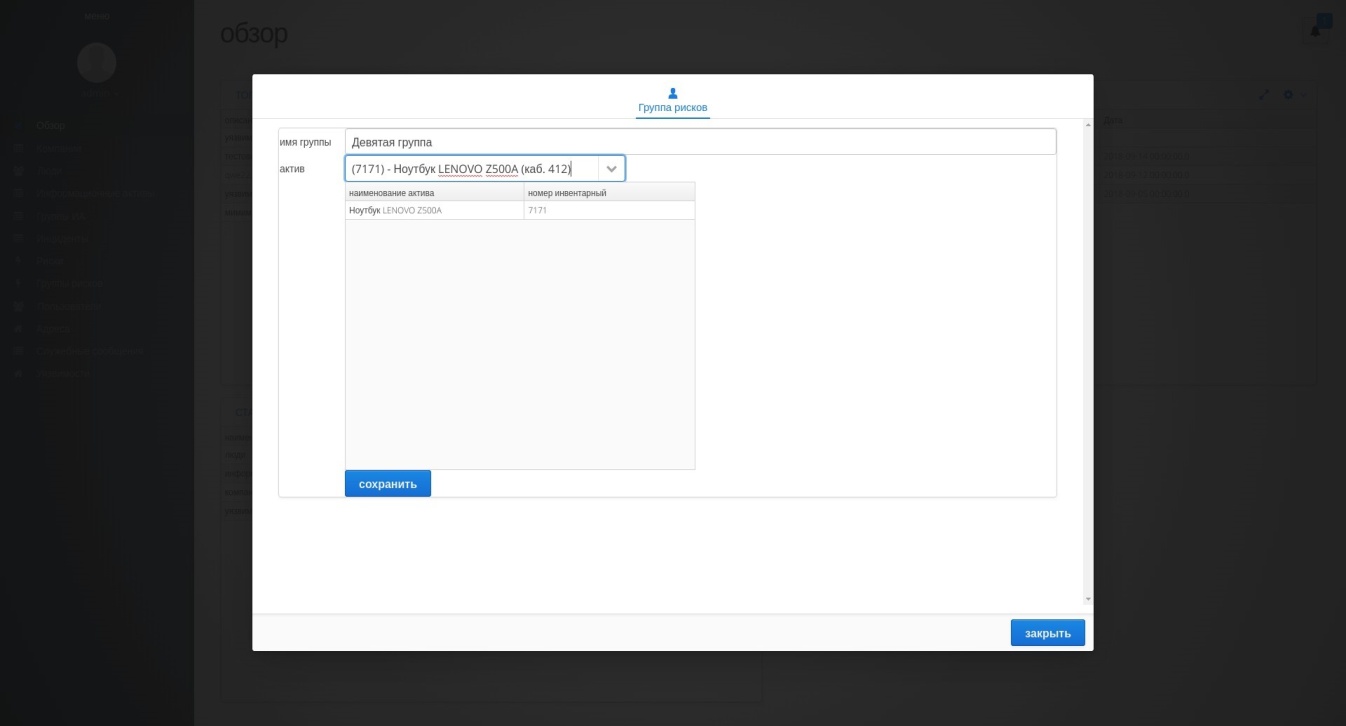


Рис. 3.7. Створення нової групи активів

Після збереження групи вона автоматично з'явиться у списку вибору груп активів.

**3.5.6 Створення вразливості.**

Для створення вразливості необхідно на таблиці вразливостей в "Форма редагування вразливості" викликати контекстне меню натисненням правої кнопки миші і вибрати "новий запис" (рис. 3.8).

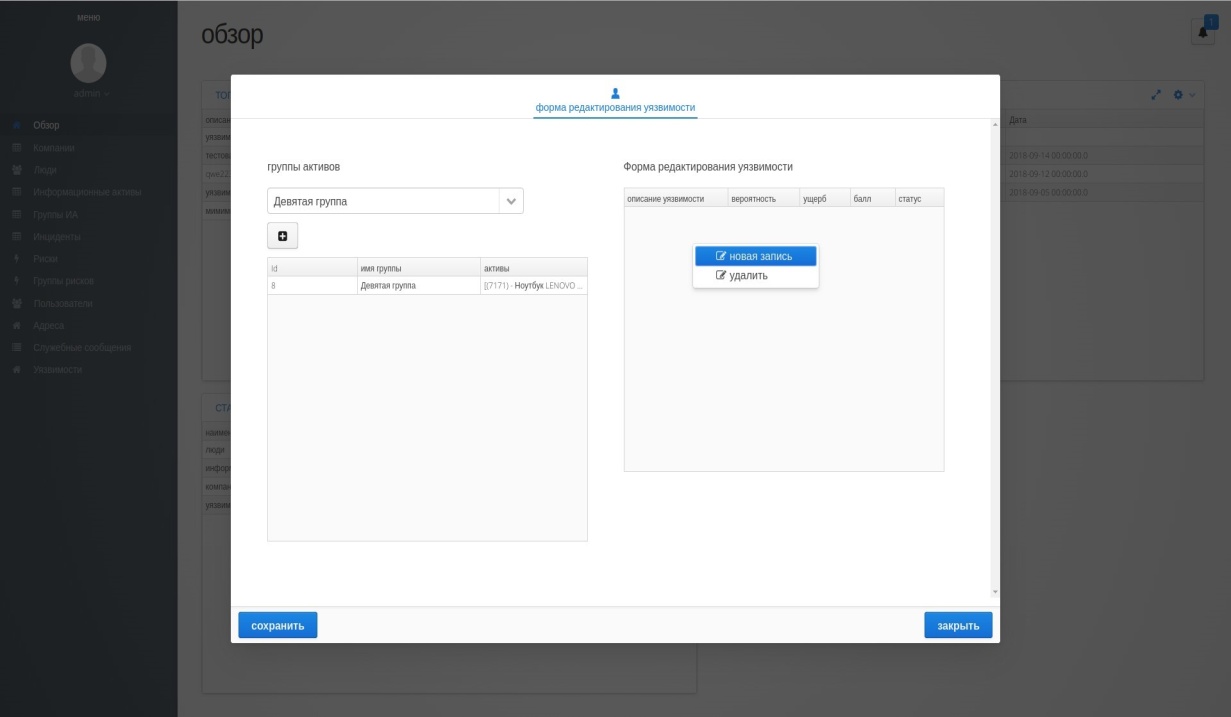


Рис. 3.8. Вікно "Форма редагування вразливості".

Після чого з'явиться запис в таблиці, яку необхідно заповнити. Для редагування доступні наступні поля "опис вразливості", "ймовірність", "збиток" (рис. 3.9.). Поля «бал» і «статус» недоступні для редагування. Поле статус доступно для редагування тільки з Dashboard.

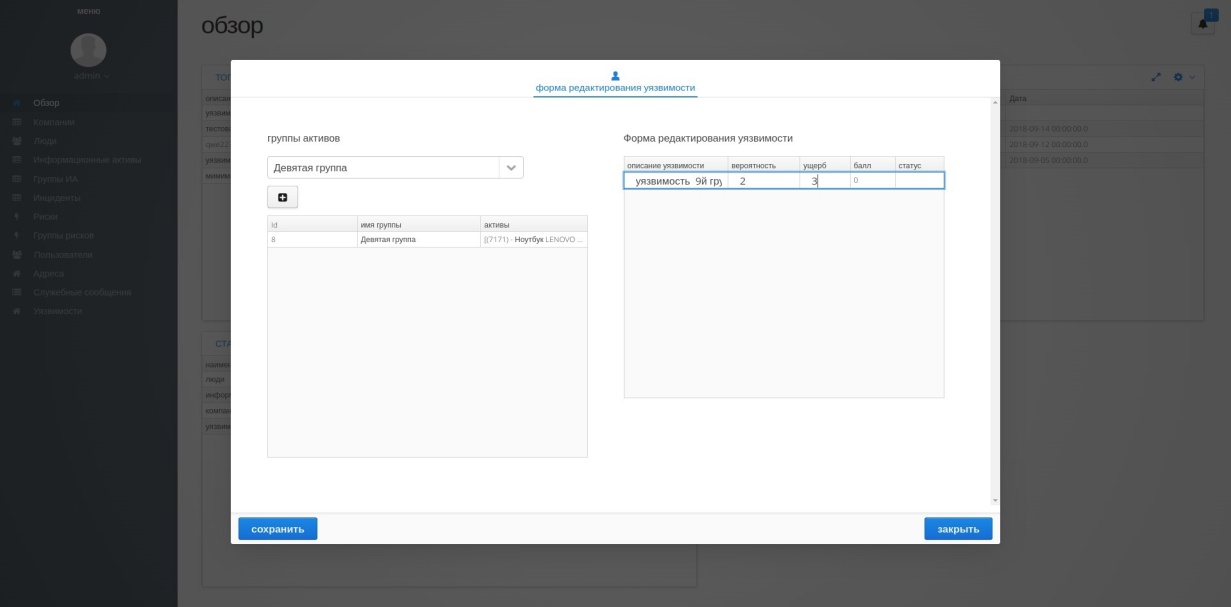


Рис. 3.9. Створення нової вразливості.

**3.5.7 Розділ "Інциденти".**

Для створення нового інциденту необхідно на головній сторінці на таблиці "Інциденти" викликати контекстне меню і вибрати пункт "новий запис" (рис. 3.10).

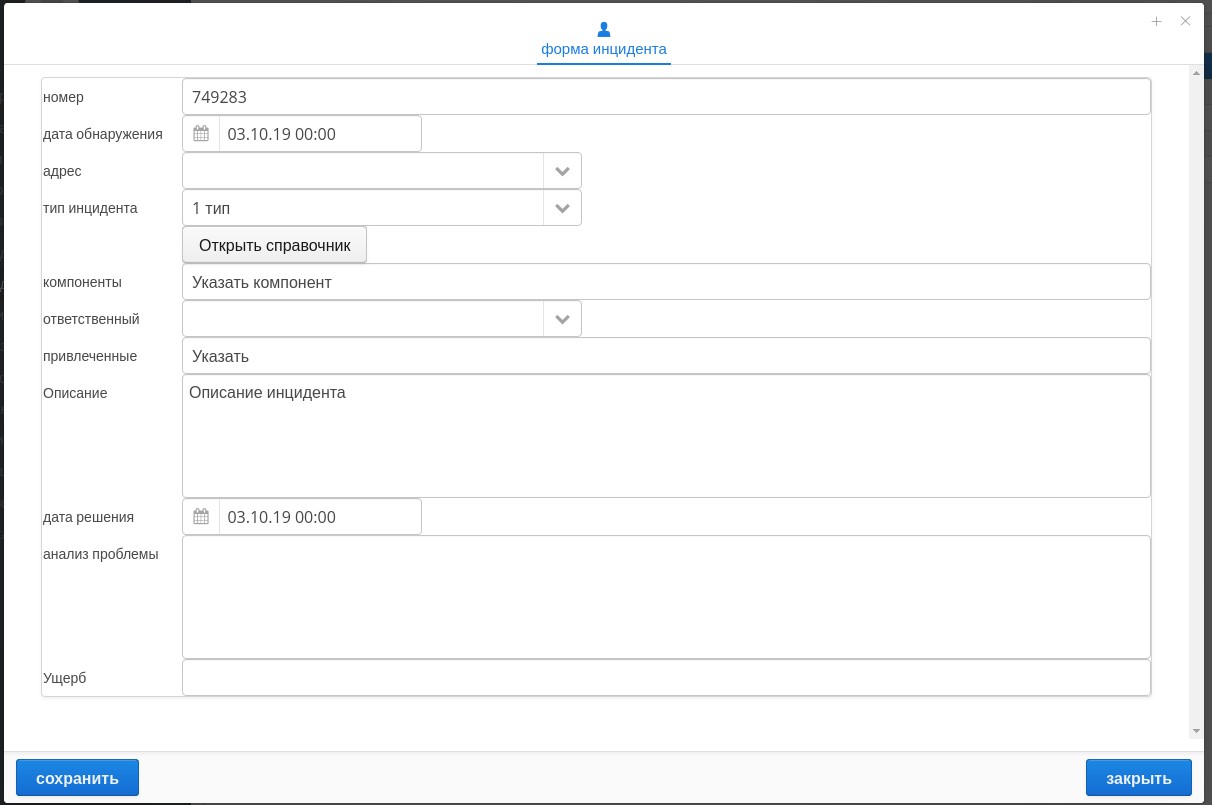


Рис. 3.10. Вікно форми "Інциденти".

Заповнивши форму необхідно натиснути кнопку "зберегти".

Перегляд реєстру інцидентів проводиться шляхом переходу по меню "Інциденти". У цьому реєстрі можна редагувати і створювати нові інциденти (рис. 311).

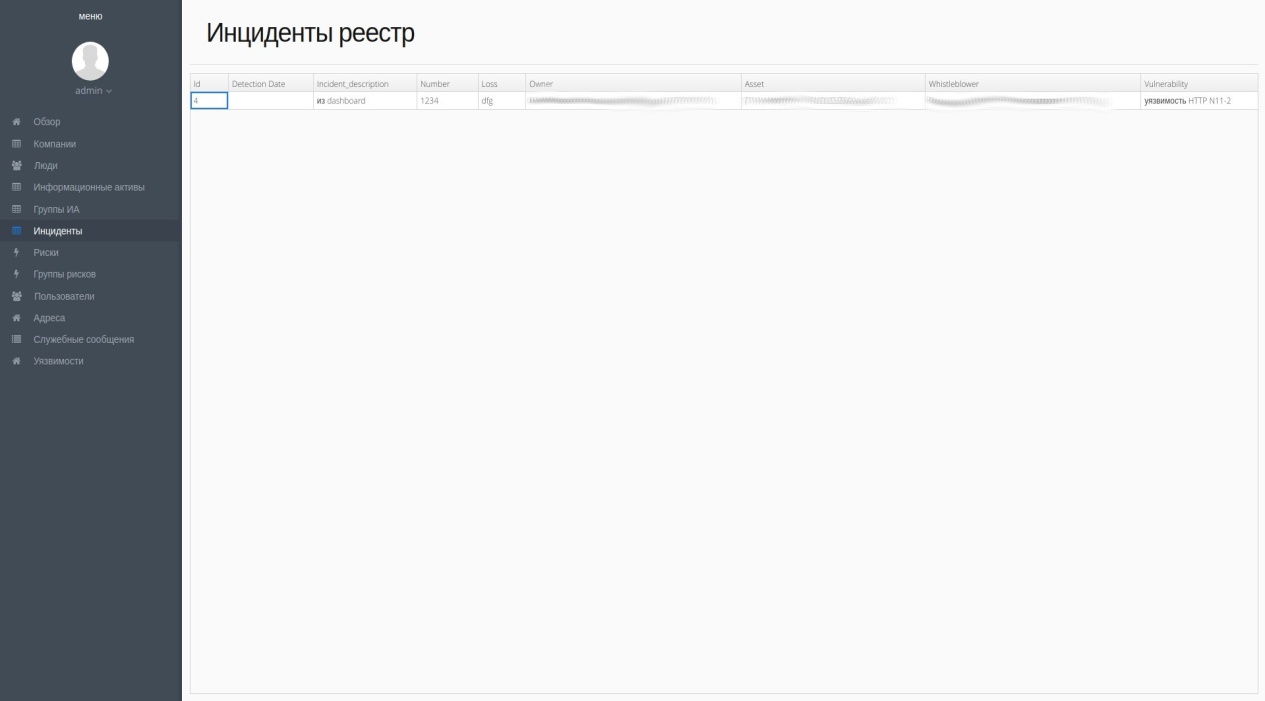


Рис. 3.11. Створення нового інциденту.

**3.5.8 Розділ "Інформаційні активи".**

У розділі "Інформаційні активи" в реєстрі необхідно викликати контекстне меню натисненням правої кнопки миші, і в випадаючому списку вибрати пункт "створити" (рис. 3.12).

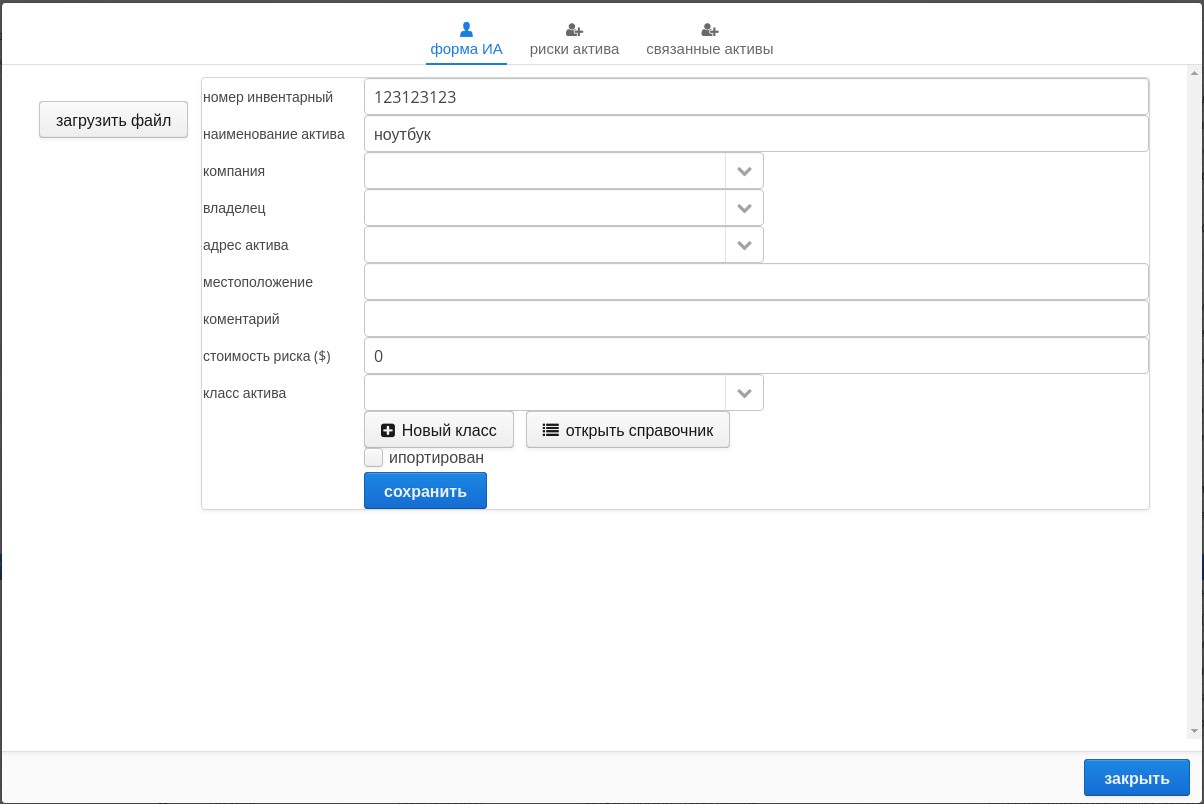


Рис. 3.12. Вікно інформаційних активів.

Після заповнення всіх полів необхідно натиснути кнопку "зберегти" для збереження запису. У вкладках "Ризики активу" і "Пов'язані активи" можна вказати відповідні дані.

Для імпорту інформаційних активів з файлу CSV необхідно в реєстрі Інформаційних активів натиснути кнопку "загрузить" (рис. 3.13).

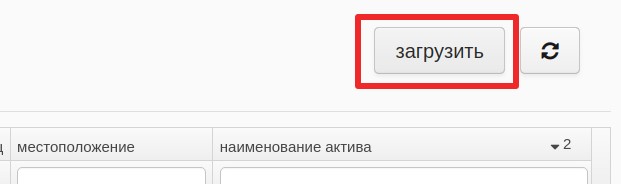


Рис. 3.13. Імпорт інформаційних активів.

Після натискання на кнопку відкриється форма схожа на форму введення активу. У цій потрібно вибрати поля для підстановки в усі активи. Після успішного парсинга файлу, готові для імпорту записи будуть відображені в таблиці форми. Для збереження записів в БД необхідно натиснути кнопку "сохранить записи в БД" (рис. 3.14).

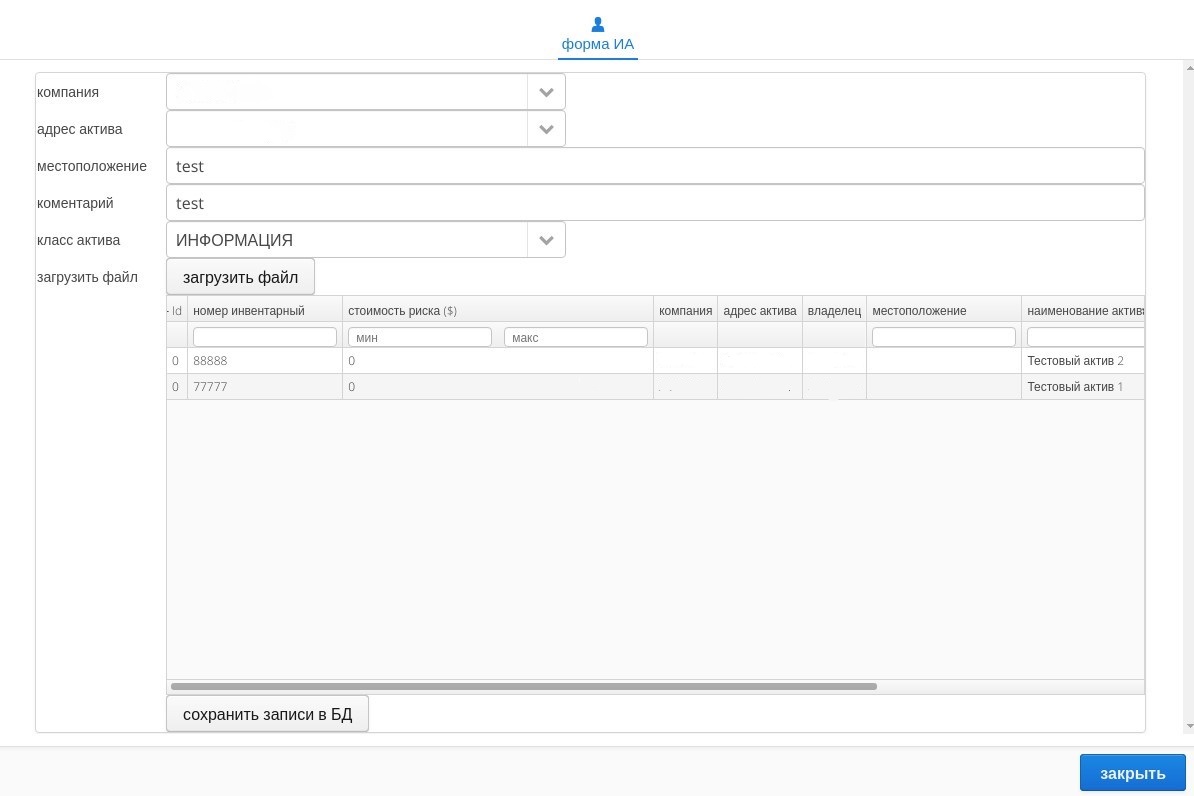


Рис. 3.14. Вікно «Збереження інформаційних активів»

Після успішного імпорту записів в БД вони будуть автоматично відображені в загальному реєстрі інформаційних активів.

**3.4 Опис коду модуля «Інформаційні Активи».**

Внесення інформаційних активів в систему вимагає побудови баз даних з великою кількістю таблиць. Робота з базами даних безпосередньо, може бути досить складною, особливо при роботі з даними відразу з декількох таблиць і при застосуванні різних фільтрів. Щоб забезпечити найкращу швидкість роботи, хорошу масштабованість в будь-якому середовищі, був використаний ORM Фреймворк [x1]. Структурна схема роботи ORM Фреймворк показана на рис. 3.15.

ORM - це абревіатура для Object Relational Mapping (Об'єктно-реляційне відображення). ORM є методикою або технікою програмування, призначена для перетворення між несумісними типами даних в об'єктно-орієнтованих мовах програмування. Суть цього досить складного визначення полягає в тому, що створюється якась абстракція - "віртуальна об'єктна база", запити до якої, перетворюються в SQL команди, тобто більше не потрібно писати SQL-запити до бази даних вручну [x1].

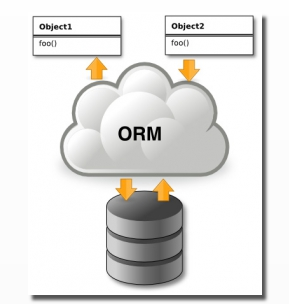


Рис. 3.15. Структурна схема роботи ORM Фреймворк [x1].

ORM дозволяє розробникам легше писати програми, які служать для подання заявки. Як структура об'єктно-реляційного картографування (ORM), Hibernate переймається стійкістю даних, оскільки це стосується реляційних баз даних (через JDBC) [x2].

Окрім власного "рідного" API, Hibernate - це також реалізація специфікації Java Persistence API (JPA). Таким чином, його можна легко використовувати в будь-якому середовищі, що підтримує JPA, включаючи додатки Java SE, сервери додатків Java EE, контейнери Enterprise OSGi тощо [x2].

Hibernate дозволяє розробити стійкі класи за природними об'єктно-орієнтованими ідіомами, включаючи спадкування, поліморфізм, асоціацію, композицію та рамки колекцій Java. Hibernate не потребує інтерфейсів або базових класів для стійких класів і дозволяє будь-якому класу або структурі даних бути стійкими [x2].

Hibernate підтримує ліниву ініціалізацію, численні стратегії отримання та оптимістичне блокування з автоматичною версією та маркуванням часу. Hibernate не вимагає спеціальних таблиць баз даних або полів і генерує значну частину SQL під час ініціалізації системи, а не під час виконання [x2].

Hibernate послідовно пропонує кращі показники порівняно з прямим кодом JDBC, як з точки зору продуктивності розробника, так і в умовах виконання [x2].

Hibernate був розроблений для роботи в кластерному сервері додатків і забезпечив високо масштабовану архітектуру. Hibernate добре масштабується в будь-якому середовищі, тому її можливо використовуйте для управління внутрішньою мережею, що обслуговує сотні користувачів, або для критично важливих програм [x2].

**3.5. Оцінка ефективності розробленого коду.**

Для поліпшення роботи СМІБ необхідно проведення робіт з оцінки та обгрунтовання різних заходів якіб забезпечили необхідний рівень захищеності інформаційних активів.

Для оцінки ефективності розробленого програмного продукту необхідно обрати критерії за якими вони будуть порівнюватися.

Перша оцінка була проведена за критеріями (рис. 3.16): надійність, захищеність, швидкість роботи, доступність.

Рис. 3.16. Кругова діаграма оцінки ефективності за першими критеріями.

Друга оцінка ефективності розробленого продукта була проведена за наступними критеріями (рис.3.17): переносимість, зручність супроводу, ефективність, зручність використання, функціональність.

Рис. 3.17. Показники покращення системи.

**3.6. Висновки по розділу.**

В розділі 3 було надано мету створення Системи «Портал ESS». На підставі задач які були поставлені при вирішенні побудови СМІБ та СУІБ. Було обозначено основні модулі які потрібно було розробити або удосконалити. Модуль обліку інформаційних активів є такий що потребує модернізації.

Детально надано налаштування модулю інформаційних активів, а також обосновано вибір техніки програмування (ORM Фреймворк) яка б дозволяла забезпечити найкращу швидкість роботи, хорошу масштабованість в будь-якому середовищі.

В розділі була проведена оцінка підвищення ефективності роботи СМІБ після модернізації модуля обліку інформаційних активів за рахунок розробленого коду.

**Висновки**

В роботі було виконано наступне:

проведено аналіз систематизованої сукупності відомостей про уразливості, загрози та атаки в інформаційних системах;

досліджено методи та засоби управління комплексними системами захисту інформації;

розроблено програмний код модуля інвентаризації інформаційних активів та надано оцінку підвищення рівня його захищеності.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Електронний ресурс Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури: http://www.dsszzi.gov.ua/dsszzi/control/ uk/publish/ Режим доступу: вільний.
2. Конахович Г.Ф. Защита информации в телекоммуникационных системах. / Г.Ф. Конахович – К.: МК-Пресс, 2014. – 334 с.
3. Шматок А.С. Методы анализа критических данных на основе машинного обучения. / А.С. Шматок, Ю.И. Финенко // ОРАЛДЫҢ ҒЫЛЫМ ЖАРШЫСЫ - №3 (174) 2019. - Оралқаласы, ЖШС «Уралнаучкнига», 2019. – С. 58-62.
4. Бурячок В. Л., Толубко В.Б., Хорошко В. О., Толюпа С.В.. «Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]». - 2015.
5. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
6. Електронний ресурс: Серчинформ https://searchinform.ru/resheniya /biznes-zadachi/zaschita-personalnykh-dannykh/model-ugroz-bezopasnosti-personalnyh-dannyh/ Режим доступу: вільний.
7. Електронний ресурс: BAE Systems: Анализа киберугроз http://www.tadviser.ru/index.php /BAE\_Systems Режим доступу: вільний.
8. Електронний ресурс: Анализ угроз информационной безопасности 2016-2017 https://www.antimalware.ru/analytics/Threats\_Analysis/ Analysis\_information\_security\_threats\_2016\_2017 Режим доступу: вільний.
9. Миленький А.В. Классификация сигналов в условиях неопределенности. М.: Советское радио, 1975. 328 с.
10. Bilmes J. A Gentle Tutorial of the EM Algorithm and its Application to Parameter Estimation for Gaussian Mixture and Hidden Markov Models / J.Bilmes; International Computer Science Institute .— Berkeley: Computer Science Division Department of Electrical Engineering and Computer Science, 1998 .— 15 с.
11. Data Analysis, Machine Learning and Applications / C.Preisach, H.Burkhardt, L.Schmidt-Thieme, R.Decker and etc.; Proceedings of the 31st Annual Conference of the Gesellschaft für Klassifikation, Albert-Ludwigs-Universität Freiburg, March 7–9, 2007 .— Berlin Heidelberg: Springer-Verlag, 2008 .— 703 p.
12. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер. – СПб.: Питер, 2003, 368 с.
13. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. - М.: Солон-Пресс, 2002
14. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning. — Springer, 2001
15. Електронний ресурс: eLibrary https://elibrary.ru/item.asp ?id=41137645/. Режим доступу: вільний.
16. Айвазян С. А., Бухштабер В. М., Енюков И. С., Мешалкин Л. Д. Прикладная статистика: классификация и снижение размерности. — М.: Финансы и статистика, 1989.
17. Вапник В. Н., Червоненкис А. Я. Теория распознавания образов. — М.: Наука, 1974.
18. Вапник В. Н. Восстановление зависимостей по эмпирическим данным. — М.: Наука, 1979.
19. Дуда Р., Харт П. Распознавание образов и анализ сцен. — М.: Мир, 1976.
20. Charu C. Aggarwal Data Mining. The Textbook. / C.A.Charu; — Springer, 2015 .— 746 p.
21. Christopher M. Bishop Pattern Recognition and Machine Learning / M.B.Christopher .— Springer, 2006 .— 758 p.
22. Clarke B. Principles and Theory for Data Mining and Machine Learning / B.Clarke, E.Fokoue, H.Zhang .— Dordrecht Heidelberg London New York: Springer, 2009 .— 793 с.
23. Engelmann B. The Basel II Risk Parameters / B.Engelmann, R.Rauhmeier; Estimation, Validation, Stress Testing – with Applications to Loan Risk Management .— Heidelberg Dordrecht London New York: Springer, 2011 .— 419 с.
24. Giudici P. Applied data mining: statistical methods for business and industry / P.Giudici .— West Sussex, England: John Wiley & Sons Ltd, 2003 .— 378 с.
25. Goodfellow I. Deep Learning / I.Goodfellow, Y.Bengio, A.Courville .— MIT: MIT Press, 2016 .— 800 с.
26. Hand D. Principles of Data Mining / D.Hand, H.Mannila, P.Smyth .— MIT: The MIT Press, 2001 .— 546 с.
27. Hastie T. The Elements of Statistical Learning Data Mining, Inference, and Prediction / T.Hastie, R.Tibshirani, J.Friedman; Second Edition .— Springer, 2017 .— 764 p.
28. Lausen B. Data Science, Learning by Latent Structures, and Knowledge Discovery / B.Lausen, S.Krolak-Schwerdt, M.Böhmer .— Berlin Heidelberg: Springer, 2015 .— 552 с.
29. McLachlan G.J. The EM algorithm and extensions / G.J.McLachlan, T.Krishnan .— New York: John Wiley & Sons, Inc., 1997 .— 288 с.
30. Nisbet R. Handbook of statistical analysys and data mining applications / R.Nisbet, J.Elder, G.Miner .— San Diego: Elsevier Inc., 2009 .— 860 с.
31. Pattern, Recognition and Machine Intelligence / Sergei O. Kuznetsov Deba P. Mandal Malay K. Kundu Sankar K. Pal (Eds.); 4th International Conference, PReMI 2011 Moscow, Russia, June 27 – July 1, 2011 Proceedings .— Springer, 2011 .— 495 p.
32. Sammut C. Encyclopedia of Machine Learning / C.Sammut, G.Webb .— NY: Springer Science+Business Media, 2010 .— 1059 p.
33. Shalev-Shwartz S. Understanding Machine Learning: From Theory to Algorithms / S.Shalev-Shwartz, S.Ben-David .— Cambridge: Cambridge University Press., 2014 .— 449 с.
34. Wang J. Encyclopedia of Data Warehousing and Mining / J.Wang; Second Edition .— Hershey: Information Science Reference, 2009 .— 2227 p.
35. Watanabe M. The EM Algorithm and Related Statistical Models / M.Watanabe, K.Yamaguchi .— NY, Basel: Marcel Dekker, Inc., 2004 .— 214 с.
36. Королев В.Ю. ЕМ-алгоритм, его модификации и их применение к задаче разделения смесей вероятностных распределений. / В.Ю.Королев; Теоретический обзор .— М.: ИПИ РАН, 2007 .— 94 с.
37. Прикладная статистика. Классификация и снижение размерности. / С.А.Айвазян, В.М.Бухштабер, И.С.Енюков, Л.Д.Мешалкин .— М.: Финансы и статистика, 1989 .— 607 с.
38. Шумейко А.А., Сотник С.Л. Интеллектуальный анализ данных (Введение в Data Mining).-Днепропетровск:Белая Е.А., 2012.- 212 с.
39. Эсбенсен К. Анализ многомерных данных / К.Эсбенсен .— Черноголовка: ИПХФ РАН, 2005 .— 160 с.
40. Годин, А. М. Статистика: учебник / А. М. Годин. – Москва: Дашков и К°, 2016. – 451 с.
41. Гореева, Н. М. Статистика в схемах и таблицах /. – Москва: Эксмо, 2017. – 414 с.
42. Едроновва Общая теория статистики / Едроновва, В.Н; Едронова, М.В.. - М.: ЮРИСТЪ, 2017. - 511
43. Елисеева, И. И. Статистика: [углубленный курс]: учебник для бакалавров / И. И. Елисеева и др.]. – Москва: Юрайт: ИД Юрайт, 2016. – 565 с.
44. Зинченко, А. П. Статистика: учебник / А. П. Зинченко. – Москва: КолосС, 2016. – 566 с.
45. Ивченко, Г.И. Математическая статистика / Г.И. Ивченко, Ю.И. Медведев. - М.: [не указано], 2016. - 329 c.
46. Лексин, В. Н. Муниципальная Россия. Социально-экономическая ситуация, право, статистика. Том 3 / В.Н. Лексин, А.Н. Швецов. - Москва: СИНТЕГ, 2017. - 992 c.
47. Ниворожкина, Л. И. Статистика: учебник для бакалавров: учебник /. – Москва: Дашков и Кº: Наука–Спектр, 2015. – 415 с.
48. Рейтлингер, Л.Р. Материалы для статистики глазных болезней, господствующих в войсках русской армии / Л.Р. Рейтлингер. - М.: С-Пб.: Богельман, 2017.- 128 c.
49. Романовский, В.И. Избранные труды, том 2. Теория вероятностей, статистика и анализ / В.И., Романовский. - М.: [не указано], 2017. - 145 c.
50. Статистика: учебник / [И. И. Елисеева и др.]. – Москва: Проспект, 2015. – 443 с.
51. Статистика и бухгалтерский учет / [А. П. Зинченко и др.]. – Москва: КолосС, 2018. – 436 с.
52. Статистика: учебно–практическое пособие / [М. Г. Назаров и др.]. – Москва: КноРус, 2018. – 479 с.
53. Статистика: учебное пособие для высших учебных заведений по экономическим специальностям / В. М. Гусаров, Е. И. Кузнецова. – Москва: ЮНИТИ–ДАНА, 2016. – 479 с.
54. Статистика: теория и практика в Excel: учебное / В. С. Лялин, И. Г. Зверева, Н. Г. Никифорова. – Москва: Финансы и статистика: Инфра–М, 2016. – 446,
55. Статистика финансов: учебник / [М. Г. Назаров и др.]. – Москва: Омега–Л, 2018. – 460 с.
56. Тумасян, А. А. Статистика промышленности: учебное пособие / А. А. Тумасян, Л. И. Василевская. – Минск: Новое знание. – Москва: Инфра–М, 2017. – 429 с.
57. Тюрин, Ю.Н. Лекции по математической статистике / Ю.Н. Тюрин. - М.: [не указано], 2017. - 992 c.
58. Харченко, Н. М. Экономическая статистика: учебник / Н. М. Харченко. – Москва: Дашков и Кº, 2016. – 365 с.
59. Экономическая статистика: учебник / [А. Р. Алексеев и др.]. – Москва: Инфра–М, 2016. – 666 с.
60. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс – М.; Феникс, 2008. – 174 с.
61. Харкевич А.А. Опознавание образов // Радиотехника. 1959. Т. 14, №5. С. 3-9.
62. Пугачев B.C. Введение в теорию вероятностей. М.: Наука, 1968. 368 с.
63. Електронний ресурс: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/ Режим доступу: вільний.
64. Шматок А.С. Методы анализа критических данных на основе машинного обучения. / А.С. Шматок, Ю.И. Финенко // ОРАЛДЫҢ ҒЫЛЫМ ЖАРШЫСЫ - №3 (130) 3019. - Оралқаласы, ЖШС «Уралнаучкнига», 3019. – С. 58-63.
65. Шматок О.С. Штучний інтелект та машинне навчання в задачах стеганоаналізу даних. / О.С. Шматок, Ю.І. Фіненко, А.Б. Єлізаров, В.А. Телющенко // Вісник Університету «Україна», Серія: «Інформатика, обчислювальна техніка та кібернетика» - №3 (33) 3019. – Київ, Університет «Україна», 3019. С.319-337.
66. Агеев А. С. Автоматизированные системы контроля защищенности объектов электронно-вычислительной техники и перспективы их развития // А. С. Агеев, Вопросы защиты информации. 2015 — №2. – 93 с.
67. Арьков П. А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации: дис…. канд. техн. наук: 05.13.19. — Волгоград, 2009. — 410 с.
68. Барзилович Е.Ю. Модели технического обслуживания сложных систем // Е. Ю. Барзилович, М.: Высшая школа, 2012 — 231 с.
69. Герасименко В. А. Защита информации в автоматизированных системах обработки данных : В 2 кн. — М.: Энергоатомиздат, 2014 – 156 с.
70. Горбатов B.C., Кондратьева Т.А. Информационная безопасность. Основы правовой защиты // В.С. Горбатов, М.: МИФИ, 2015 – 320 с.
71. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов // Ф. М. Курилов, Технические науки: теория и практика: материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). — Чита: Издательство Молодой ученый, 2016. — 112 с.
72. Нестеров С. А. Анализ и управление рисками в сфере информационной безопасности: Учебный курс. — СПб.: СПбГПУ, 2007. — 47 с. Отчет «Исследование текущих тенденций в области информационной безопасности бизнеса» [Электронный ресурс] // Лаборатория Касперского. — 2017. URL: http://media.kaspersky.com/ (дата обращения: 23.03.2017).
73. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа // А. Ю. Щеглов, СПб: Наука и техника, 2014. — 384 с.
74. Ярочкин В.И. Безопасность информационных систем // В. И. Ярочкин, М.: Ось, 2015  — 320 с.
75. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М: Горячаялиния-Телеком, 2008. 452 с.
76. Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control // IEEE Transactions on Systems, Man and Cybernetics. 1985. Vol. SMC-15, no 1. P. 116-132. DOI: 10.1109/TSMC.1985.6313399
77. Хайкин С. Нейронные сети: полный курс: пер. с англ. М.: Издательский дом «Вильямс», 2006. 1104 с.
78. Булдакова Т.И. Нейросетевая защита ресурсов автоматизированных систем от несанкционированного доступа // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 5. DOI: 10.7463/0513.0566210
79. Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Г.Ф., Воскресенский С.И. К моделированию адаптивной системы информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2004. № 4. С. 25-31.