МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук

«_____»_____ 20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Експертна система управління ІБ на підприємстві середнього бізнесу

Автор: А.М. Чечуга

Науковий керівник: д.т.н., проф. С.В. Толюпа

Нормконтроллер: д.т.н., проф. С.В. Толюпа

Київ 2020

ВСТУП

Актуальність. На сьогоднішній день у зв’язку з стрімким зростанням кількості і масштабів підприємств, зростають і об'єми інформації, котрі циркулюють в межах інфраструктури підприємства, тож має місце і інформаційна безпека. Розробка експертної системи для підприємства середнього бізнесу важлива задля того щоб підвищити ефективність СЗІ за рахунок зниження витрат часу на виконання процесів забезпечення ІБ і прийняття управлінських рішень, на основі експертних систем.

Для розробки ефективної експертної системи управління ІБ на підприємстві потрібно провести аналіз і визначити усі бізнес-процеси, які наявні на підприємстві, визначити відповідальних осіб за них. Визначити усі інформаційні активи компанії, провести оцінку їх вразливості до різних типів загроз. На базі цієї оцінки розробити програмний модуль для експертної системи управління інформаційною безпекою на підприємстві середнього бізнесу.

Відомі підходи до вирішення поставленої задачі. На сьогоднішній день існує безліч інструментальних засобів і методик задля розробки експертних систем управління ІБ на підприємстві. Це такі продукти, як COBRA, CRAMM, Calleo Secura, OCTAVE, Risk Watch, vsRisk, Авангард. Проте всі ці продукти мають певні недолікі, деякі застаріли і не відповідають актуальним потребам бізнесу. Деякі мають високу собівартість, далеко не кожен середній бізнес може собі це дозволити. Інші ж мають дуже простий і базовий інтерфейс і реалізовані з базовим методо оцінки, що часто не покриває потреби підприємств.

Метою роботи є розробка експертної системи управління інформаційною безпекою на підприємстві середнього бізнесу.

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

– Огляд досліджень та нормативно-правової бази в галузі інформаційної безпеки та експертних систем;

– побудова системи управління інформаційною безпекою на підприємстві середнього бізнесу;

– розробка програмного модулю для системи управління інформаційною безпекою на підприємтві середнього бізнесу.

Галузь застосування. Розроблений програмний модуль відноситься до галузі інформаційної безпеки і може бути використаний для підвищення рівня інформаційної безпеки та підвищення економічного клімату компанії.

Об'єктом дослідження є процес управління інформаційною безпекою на підприємстві середнього бізнесу.

Предметом дослідження є методи і моделі управління інформаційною безпекою, що грунтуються на застосуванні експертних систем.

Методи дослідження базуються на основі методу теорії нечітких множин, теорії алгоритмів, теорії управління, теорії обчислювальних систем і мереж, теорії графів, стандартів інформаційної безпеки.

Новизна одержаних результатів полягає в наступному:

- розроблена експертна система для підприємства середнього бізнесу на основі розробленої концепції забезпечення інформаційної безпеки. Це дає можливість здійснення оперативного і стратегічного управління інформ.безпекою, з огляду на специфіку діючої в організації системи захисту інформації та IT інфраструктури, збільшуючи ефективність системи захисту інформації.

Практична цінність роботи полягає в покращені технології забезпечення захисту інформації на підприємстві середнього бізнесу шляхом впровадження експертної системи управління інформаційною безпекою.

Апробація. Основні положення роботи доповідалися та обговорювалися:

- Чечуга А.М. Засіб контролю трафіку у комп'ютерних мережах: Прикладні наукові розробки: тези доп. XVI Наук.-практ. конф. з міжнар. участю, м. Прага, 22-30 липня 2020 р. / Видавництво "Education and Science", Прага, 2020. с. 21-23.
- Чечуга А.М. Автоматизація процесу управління інцидентами інформаційної безпеки / Чечуга А.М., Толюпа С.В., Шестак С.В., Кулько А.А. // Прикладні системи та технології в інформаційному суспільстві: тези доп. IV Наук.-практ. конф. з міжнар. участю, м. Київ, 30 вересня 2020 р.. с. 215-221.

РОЗДІЛ 1. ОГЛЯД ДОСЛІДЖЕНЬ ТА СТАНДАРТІВ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЕКСПЕРТНИХ СИСТЕМ

1.1. Дослідження в галузі розробки експертних систем управління інформаційною безпекою

Предметом дослідження українських та інозмених вчених є складові елементи управління інформаційною безпекою та проблеми забезпечення інформаційної безпеки. Побудови експертних систем, різні аспекти управління, забезпечення інформаційної безпеки, побудови експертних систем, застосування інтелектуальних систем в окремих частинах інформаційної безпеки, оцінки захищеності інформаційних систем, розглядаються в працях відомих українських та зарубіжних вчених, таких як: Ю.І. Хлапонін [1,2], О.В. Бойченко [3], О.В. Бучка , С.С. Бучик [4], С.Я. Довбня [5], О.А. Журан [6], О.А. Бурдин [7], Г.П. Жигулін [8], О.Ю. Гаценко, Ю.А.Печеневскій , М.Б. Будько [9], В.Г. Швед, Н.Н. Безруков, Н.Г. Милославська, М.Ю. Сенаторів, С.В. Симонов [10,1й], А.І. Толстой, О.Ю. Домарева, А.А., Воробйова, Л.К. Бабенко, О.О. Анісімов [1ц], Ю.А. Печеневський, А.А. Малюк, А.Г. Корченко, Е. Вілсон [13], Д. Уотермен [14], Джарратано Дж., Райли Г. [15].

Найповніший опис і рощгляд застосування експертних систем при реалізації систем підтримки прийняття рішень на підприємствах мають місце в роботах Ю.І. Хлапонін [1,2], Бурдин [7], С.Я. Довбня [5], С.М. Суменкова, М.С. Суменкова [16], А.Б. Петровського , В.Ф. Хорошевського [17], К. Таунсенда, Д. Фохт [18].

Принципи побудови систем управління розгорнуто розглянуті в роботах Д. Джарратано, Г. Райлі [15].

Підходи реалізації систем підтримки прийняття управлінських рішень викладені в статтях Е.А. Трахтенгерц [19].

Деякі дослідники [5] відмічають, що основні труднощі в оцінці загроз полягають у великому об’ємі вхідної інформації для оцінки загроз. Тому виникає необхідність у створенні інтелектуальних систем для обробки та аналізу такої інформації. Інша складність полягає у тому, що існуючі експертні системи мають загальний характер і не є орієнтованими на спеціальних замовників.

1.2 Огляд міжнародних стандартів в галузі інформаційної безпеки

1.2.1 Огляд стандартів ISO в галузі інформаційної безпеки

Управління інформаційною безпекою досить широко обговорювана тема в міжнародному співтоваристві. Доказом цього факту є наявність серії міжнародних стандартів [20, 21, 22, 23, 24, 25, 26, 27, 28, 29], розроблених загальними зусиллями Міжнародної організації за стандартами і Міжнародною електротехнічною комісією.

Робота над стандартами була розпочата в 1999 році і в підсумковому варіанті документи побачили світ на початку 2000 року, у вигляді першої частини, в якій на досить простому рівні описувалася проблематика сучасних тенденцій розвитку інформаційної безпеки, що склалася і давалися практичні рекомендації по здійсненню впровадження механізмів управління інформаційної безпеки. Через декілька років, в 2002 році була випущена друга частина документу, що описує загальну специфікацію пропонованих першою частиною документу рішень, потім послідували супутні документи серії. Слід зазначити, що серія стандартів продовжує розвиватися, а ряд стандартів, що входять в серію, постійно переглядається і оновлюється. Підсумкова версія другої частини документу отримала широку популярність і схвалення в міжнародному співтоваристві, результатом цих досліджень послужив вихід стандарту ISO\IEC 27001. В процесі проведення

дослідження, стандартам була приділена особлива увага. Зокрема, перший стандарт описує основні принципи організації управління інформаційної безпеки, для організацій різного роду діяльності, тоді як другий стандарт більше приділяв увагу безпосереднім механізмам управління інформаційною безпекою, з послідовним розбиттям кроків по реалізації кожного із запропонованих механізмів.

ISO\IEC 27000 є свого роду передмовою до інших документів серії, основне призначення якого зводиться до опису сфери впливу кожного із стандартів, а також опису загальних принципів і причин виникнення стандарту. Дається керівництво по використанню змісту стандартів при введенні системи менеджменту інформаційної безпеці в організації, а також опис основних процессных складових і актуальності впровадження цієї системи. Згідно із структурою ISO\IEC 27000, сімейство (серія) стандартів представляє з себе логічно пов'язані документи, систему менеджменту інформаційній безпеці. Схема зв'язків документів, що входять в серію, представлена на малюнку 1.1. Основною метою цієї серії є введення системи менеджменту інформаційній безпеці в організаціях різної величини і роду діяльності. У додатку до документу представлені словестные форми вираження стандартів категорированный перелік термінів по інформаційній безпеці, вживаних в стандарті.

- ISO\IEC 27000 "Системи менеджменту інформаційній безпеці.
- Загальний огляд і термінологія"
- ISO\IEC 27001 "Система менеджменту інформаційній безпеці. Вимоги"
- ISO\IEC 27006 "Вимоги для органів 0000ї що забезпечують аудит і сертифікацію систем менеджменту інформаційній безпеці"
- ISO\IEC 27002 "Зведення правило по управлінню захистом інформації"
- ISO\IEC 27003 "Керівництво по реалізації системи менеджменту інформаційній безпеці"
- ISO\IEC 27004 "Менеджмент інформаційної безпеці. Виміри"

- ISO\IEC 27005 "Управління рисками інформаційній безпеці"
- ISO\IEC 27007 "Керівництво для аудитора Системи менеджменту інформаційної безопаности"
- ISO\IEC 27799 "Інформатика в охороні здоров'я. Менеджмент інформаційної безпеці за стандартом ISO/IEC 27002"
- ISO\IEC 270011 "Керівні вказівки по управлінню захистом інформації організацій, що пропонують телекомунікаційні послуги, на основі ISO/IEC 27002"

Схема зв'язків цих документів представлена на Рисунку 1.1.

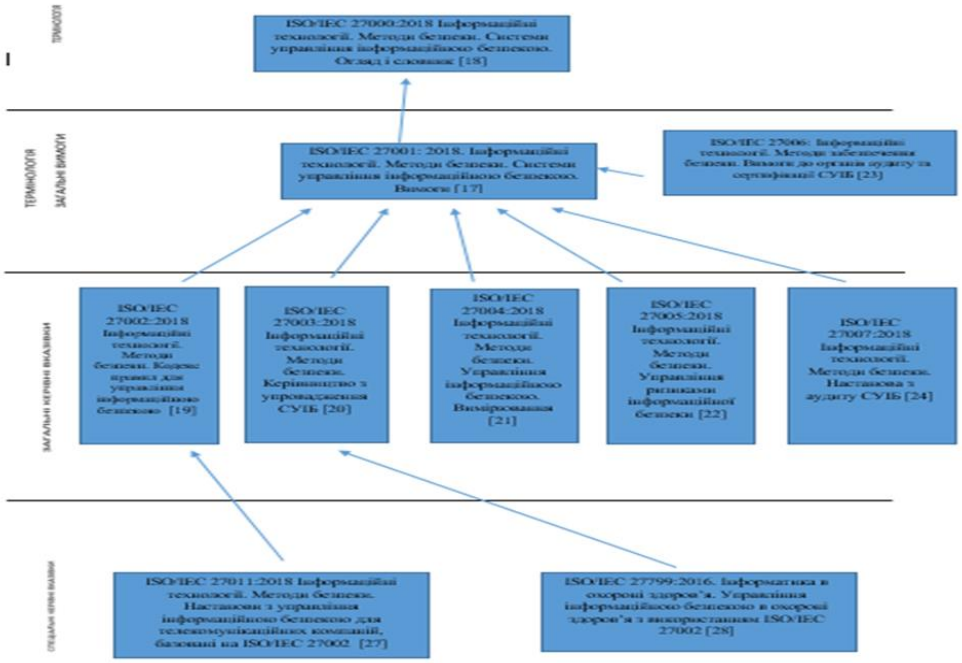

Рис. 1.1 – Стандарти серії ISO/IEC 27000 в галузі ІБ та їх взаємозв’язок.

Згідно з положеннями ISO\IEC 27001 система менеджменту інформаційної безпеки повинна мати процессний характер, що дотримується положенням циклу Демінгу - Шухарта, що полягає в послідовності дій з планування процесу, його здійсненні і подальшої перевірки, після чого повинна йти зміна що полягає в плавному перегляді підходів і актуалізації уваги на подальше планування, після чого цикл повторюється.

Відповідно до вимог стандарту, керівництво організації повинне визначити межі дії систем управління інформаційною безпекою, після чого сформувати політику управління інформаційною безпекою, що формує концептуальні характеристики бізнесу організації, сукупність її активів і вживаних інформаційних технологій. Наступним ключовим етапом має бути оцінка ризиків і вибір методу їх обробки, з метою формування єдиної системи поглядів на питання забезпечення і управління інформаційною безпекою в організації. Подальшим етапом повинно служити виявлення ризиків, згідно з вибраним методом, відповідним для конкретної організації. Виявлення ризиків передбачається здійснювати за допомогою формування переліку активів і їх власників, з метою виявлення слабких місць, уразливості яких можуть дати поштовх для реалізації загроз інформаційної безпеки, в сукупності з виявленням деструктивних дій на ці активи з точки зору інформаційної безпеки.

Наступним проміжним етапом є оцінка виявлених ризиків і формування стратегії управлінням ними, що полягає в:

− зміні параметрів захисту і\чи управління;

− прийнятті ризиків, у разі задоволення умовам (раніше за описувану) політики;

− позбавлення від ризиків;

− покладання відповідальності за ці риски на сторонні організації, або передача ризиків.

В результаті прийняття певної стратегії управління рисками, згідно стандарту, повинне послідувати зниження рівня ризику до прийнятного рівня - залишкового ризику. Таким чином, система управління інформаційною безпекою організації є документованою і готовою для впровадження.

Згідно з положеннями ISO\IEC 27001 процес реалізації і експлуатації системи менеджменту інформаційної безпеки повинен полягатимуть в:

1. Формулюванню плану обробки ризиків.

2. Реалізації плану обробки ризиків.

3. Формуванні і застосуванні засобів управління.

4. Оцінці ефективності прийнятих засобів управління.

5. Підготовці і здійсненні плану підвищення обізнаності персоналу.

6. Управлінні діяльністю системи менеджменту інформаційної безпеки.

7. Управлінні ресурсами системи менеджменту інформаційної безпеки.

8. Впровадженні в дію систем виявлення інцидентів інформаційної безпеці.

Таким чином, згідно з циклом Демінга - Шухарта, вищеописані дії являються процесами планування і здійснення, після яких повинні слідувати процеси перевірки і перегляду попередніх дій (вдосконалення), що і описує що залишилася частина стандарту. Особлива увага приділяється процесам документування вимог і політик організації в області інформаційної безпеки і їх захисту, а також формалізації механізмів реагування на інциденти інформаційної на інциденти інформаційної безпеки спільно з повсюдним "Управлінням записами", яке має на увазі постійне ведення журналів, протоколів і форм дозволу доступу, пов'язаних як з активами і їх рисками, так і з процесами забезпечення інформаційної безпеки організації. Також варто відмітити істотне акцентування уваги змісту документу на питання вдосконалення системи менеджменту інформаційної безпеки. Згідно з даними акцентам вдосконалення повинне здійснюватися за результатами проведення окремою процедури - власного аудиту системи, метою якого є перевірка відповідності системи бізнес вимогам, ефективності механізмів управління інформаційної безпекою і коректності виконання функцій захисту.

Результатом такої процедури має бути аналітичне укладення о можливості поліпшення, доповнення або видозміни системи, сприяюче подальшому вдосконаленню і розвитку системи управління інформаційної безпекою. У додатку до стандарту дається перелік додатків, основна мета яких - спроба формалізованого представлення цілей і засобів управління інформаційної безпекою.

Свого роду логічним продовженням вищеописаного стандарту, являється стандарт ISO\IEC 27002. По суті цей стандарт дає детальніший опис дій представлених в 27001, проте що розширює зону своєї дії до опису процесів управління активами, описи послідовності прийому в штат і підбору нові співробітників, з

метою виконання вимог по інформаційній безпеці і послідовності дій у разі припинення подальшої співпраці з співробітниками організації. Також окрема увага приділена таким аспектам як фізична і екологічна безпеці, включаючи захист периметра, устаткування, співробітників від зовнішніх екологічних загроз, розкриваючи особливості процесів утилізації використаних носіїв інформації і устаткування, а також їх повторного використання.

Таким чином ISO\IEC 27002 формує зведення правил управління інформаційною безпекою, послідовно описуючи дії, представлені в ISO\IEC 27001. Особливе увага стандарту приділяється процедурам управління засобами зв'язку і операцій що полягають в:

1. Формалізації процедур експлуатації IT устаткування організації, включаючи:

a. фіксація змін устаткування;

b. формалізацію обов'язків персоналу;

c. розділення обов'язків персоналу;

d. розмежування засобів:

i. розробки;

ii. випробувань;

iii. експлуатації.

2. Визначенні механізмів управління надання послуг третім особам включаючи:

a. Здійснення надання послуг третім особам;

b. Контроль за процесом надання послуг третім особам;

c. Аналіз послуг, що надаються, третім особам і способів їх надання;

d. Фіксація змін умов надання послуг третім особам.

3. Плануванні реалізації і здійснення приймання нових систем, включаючи управління продуктивністю систем, що вводяться, і формування способів їх приймання.

4. Захисту від шкідливого коду, за допомогою описуючи механізмів і засобів захисту від цих дій.

5. Формалізації процедури і здійснення процесів резервного копіювання інформації.

6. Формалізації правил поводження з машинними носіями інформації і засобами захисту мережевої інфраструктури.

7. Визначенні правил здійснення інформаційного обміну як усередині організації, так і при зовнішній взаємодії.

8. Описі концептуальних основ захисту інформації при здійсненні і\чи використанні послуг електронної торгівлі.

9. Описі принципів ведення контрольних журналів подій і їх захисту. Процеси розмежування і управління доступом є одними з засадничих в забезпеченні захисту інформації, що у черговий раз показується одним з найдетальніше описаних розділів стандарту - "Управління доступом". Згідно положенням стандарту, управління доступом розділене по наступних логічних компонентам:

1. Формування політики управління доступом в організації, що формалізує загальне зведення поглядів і вимог до управління доступом.

a. Управлінні доступом користувачів, включаючи:

i. Реєстрацію і облік активності користувачів в системі.

ii. Управління привілеями користувачів в системі.

iii. Організацію парольної політики і управління паролями користувачів.

iv. Аналіз діючих систем і привілеїв користувачів в них.

2. Формування загального переліку прав і обов'язків користувачів систем організації, включаючи базові принципи захисту робочих місць.

3. Управління доступом в мережах зв'язку, включаючи:

a. Управління зовнішніми з'єднаннями і правилами аутентифікації користувачів.

b. Захист видалених з'єднань.

c. Управління мережевою інфраструктурою.

4. Управління доступом до операційної системи, включаючи:

a. Обмеження часу активності користувачів.

b. Введення ліміту дії робочої сесії.

c. Систему управління паролями і ідентифікацією\аутентифікацією користувачів на робочих місцях.

d. Процедури забезпечення безпеки інформації при вході в системи організації

5. Управління доступом до інформації і додатків, включаючи базові принципи обмеження доступу до інформації і ізоляції найбільш важливих систем.

6. Формалізація принципів обробки інформації за допомогою мобільний і теле-пристроїв.

Завершальна частина документу містить в собі базовий набір дій з дотриманню вимог до інформаційної безпеки при придбанні, розробці і супроводі інформаційних систем організації. Виявлення і контроль інцидентів інформаційній безпеці організації в цілому і системі захисту інформації зокрема.

Останні глави документу містять дуже просторові рекомендації по забезпеченню безперервності бізнесу і ролі систем менеджменту інформаційної безпеки в даному процесі, а також поверхневий опис процедур перевірки відповідності юридичним вимогам і внутрішнім політикам, і стандартам в області захисту інформації що діє в організації.

Таким чином, підводячи підсумки аналізу міжнародної нормативної документації по питанням управління інформаційною безпекою можна зробити висновок, що незважаючи на наявність формалізованих принципів побудови систем управління інформаційної безпекою, розмитість формулювань, поверхневість опису ряду істотних аспектів в питаннях управління інформаційною безпекою, а також відсутність обліку специфіки діяльності організацій в умовах сучасних тенденцій розвитку підприємств в інформаційно-телекомунікаційній сфері зводить необхідність і доцільність застосування положень цих нормативних документів до нуля.

1.2.2 Огляд стандарту COBIT

CoBiT (Control Objectives for Information and Related Technology) - відкритий IT-стандарт, який в свою чергу містить ряд документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою. Історія COBIT почалася в 1996 році, в цей час ISACA (Асоціація аудиту і контролю інформаційних систем), створена в 1969 році випустила першу версію методології оцінки IT. Зараз COBIT має зв'язок з іншими стандартами в тому числі і з стандартом ISO/IEC 27000.

Стандарт сприяє чіткій координації дій IT-департаменту та керівництва компанії, об'єднує в собі ряд інших стандартів, що дозволяє на високому рівні якості отримувати інформацію про стан IT та управляти цілями і задачами IT.

Завдання COBIT полягає в ліквідації розриву між керівництвом компанії з їх баченням бізнес-цілей і IT-департаментом, що здійснює підтримку інформаційної інфраструктури, яка повинна сприяти досягненню цих цілей.

В COBIT детально описані цілі і принципи управління, об'єкти управління, чітко визначені всі IT-процеси (завдання), що протікають в компанії, і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації. В описі IT-процесів також приведені практичні рекомендації по управлінню IT-безпекою [30].

Весь матеріал COBIT 5 будується на постулатах – принципах. Таких принципів п’ять (Рисунок 1.2):

- відповідність вимогам зацікавлених сторін;
- комплексний погляд на підприємство;
- застосування єдиної інтегрованої методології;
- забезпечення цілісності підходу;
- поділ керівництва та управління.

1.2.3 Огляд стандарту ITIL

ITIL перекладається як бібліотека інфраструктури IT (бібліотека інфраструктури інформаційних технологій). Бібліотека ITIL містить повний та детальний звіт найкращих спеціалістів, які практикують. Бібліотека ITIL з'явилася в 1980-х роках за завданням британського уряду.

На сьогоднішній день більше 10 000 компаній по всьому світу використовують ITIL для управління IT.

TIL v. 3 міститься вже лише 5 книг:

- Стратегія послуги (англ. англ. Service Strategy),
- Проектування послуги (англ. Service Design),
- Перетворення послуги (англ. Service Transition),
- Експлуатація послуги (англ. Service Operation),
- Постійне удосконалення послуги (англ. Continual Service Improvement).

Крім того, у цю редакцію увійшли ще дві книги: «Огляд ITIL» та «Карманний довідник», а також довідник додаткових «незрозумілих» рекомендацій.

Переваги ITIL полягають в наступному: використання передового досвіду і перевірених знань; спрямованість діяльності IT на вирішення завдань бізнесу; використання IT служби постачальниками послуг IT для бізнес-підрозділів; регламентування діяльності угодою IT про рівень послуг; стандартизація роботи персоналу IT; спрямованість на забезпечення оптимальної якості послуг IT для споживачів; використання підходів менеджменту якості в управлінні сервісами IT; можливість підтвердження вартості сервісу IT на підставі угоди про рівень обслуговування.

1.2.4. Формування концептуальних принципів управління інформаційної безпекою

Грунтуючись на результатах проведеного аналізу міжнародної нормативно-правовій документації [20-29], у рамках дослідження були визначені основні напрями в області забезпечення інформаційної безпеки, в організаціях різного роду діяльності. До таких напрямів в організаціях різного роду діяльності відносяться:

1. Забезпечення безперервності роботи інформаційних систем і информационно-телекомунікаційних сервісів.

2. Забезпечення моніторингу, виявлення і реагування на події інформаційної безпеці.

3. Забезпечення інформаційної безпеки на різних етапах розвитку

інформаційних систем, а також підтримка і продовження життєвих циклів інформаційних систем організації.

4. Забезпечення інформаційної безпеки при здійсненні роботи з співробітниками організації, перевищення їх кваліфікації і загальної компетенції по питанням інформаційної безпеки;

5. Забезпечення інформаційної безпеки при здійсненні інформаційного обміну і взаємодії з третіми сторонами;

6. Забезпечення раціонального розмежування прав доступу до інформації і інформаційним системам користувачів організації, а також подальшого контролю за цим процесом.

Ці напрями в забезпеченні захисту інформації є основними, і будь-який процес у рамках діяльності по захисту інформації може бути до них віднесений, таким образом вводячи єдину систему класифікації діяльності по забезпеченню інформаційній безпеці. Необхідність пропорційного розвитку кожного з цих напрямів обумовлюється їх взаємозв'язаною. Відсутність належного рівня розвитку одного з напрямів, в порівнянні з іншими, неминуче приведе до нераціонального

і слабоэффективному використанню ресурсів системи захисту інформації, а також до фінансовим втратам з боку організації, не кажучи вже про збільшення вірогідності реалізації загроз інформаційної безпеки і супутньому збільшенню рівня ризику для активів організації.

Враховуючи явний процессное розподіл діяльності цих напрямів, а також асоційовану децентралізацію їх реалізації, забезпечення своєчасного і раціонального управління цими процесами є одним із засадничих питань сучасною системи захисту інформації . Управління цими напрямами дозволить істотно спростити реалізацію механізмів системи захисту інформації, простежити за планомірністю розвитку кожного з напрямів і дасть можливість грамотно перерозподілити матеріальні ресурси між напрямами, що допоможе істотно збільшити ефективність реалізованих механізмів захисту інформації при збереженні поточного рівня витрат організації на захист інформації.

Таким чином, управління процесами забезпечення інформаційної безпеки є важливою, невід'ємною складовою будь-якої системи захисту інформації в кожній організації.

1.3. Визначення основних напрямів управління інформаційною безпекою в організаціях різного роду діяльності

Побудова моделі управління інформаційною безпекою повинна дотримуватися загальноприйнятих концептуальних принципів, закладених при побудові будь-хто системи захисту інформації. Відповідно за тенденціями у сфері забезпечення захисту інформації, метод управління інформаційною безпекою повинен мати наступні концептуальні принципи:

− законність;

− системність;

− процессность;

− комплексність;

− безперервність;

− спадкоємність і безперервність вдосконалення;

− розумна достатність;

− персональна відповідальність;

− мінімізація повноважень;

− наукова обгрунтованість і технічна, що реалізовується;

− обов'язковість контролю.

Під принципом законності передбачається створення моделі управління інформаційною безпекою, її реалізація і експлуатація відповідно до того, що діє місцевим законодавством в області інформаційних технологій і інформаційної безпеки, інших нормативних актів, затверджених органами державної влади і управління в межах їх повноважень, а також локальними организационно-распорядительными документами, прийнятими усередині організації. У процесі здійснення цього концептуального принципу користувачі і обслуговуючий персонал організації повинні мати уявлення про відповідальність за правопорушення в сфері інформаційній безпеці, а також бути попередженими, що своїми діями вони можуть не лише нести матеріальну і адміністративну відповідальність, але і кримінальну

Під принципом системності передбачається такий підхід до створення моделі управління інформаційною безпекою, який враховуватиме усі взаємозв'язані взаємодіючі елементи, умови і чинники, що змінюються в часі, істотно значимих для розуміння і рішення проблем управління усіма напрямами інформаційній безпеці в організації. В процесі здійснення даного концептуального принципу особливу увагу слід звернути на взаємодію структур і фахівців із захисту інформації, а також концентрація і аналіз наявних в їх розпорядженні даних, з метою найбільш раціонального використання елементів системи, а також моніторингу і обліку чинників і умов, що впливають на інформацію.

Під принципом процессности передбачається відособлене вивчення і структуроване розбиття усіх заходів по забезпеченню інформаційної безпеці, реалізованих і\чи що реалізовуються в організації. В процесі здійснення цього концептуального принципу необхідно приділити особливу увагу деталізації опису кожного із складених процесів інформаційної безпеки, з метою формування найбільш ефективних механізмів управління ними. Під принципом комплексності передбачається використання методів і засобів управління і контролю інформаційної безпеки, що означає погоджене застосування різнорідних засобів при побудові цілісної системи управління інформаційної безпекою, що реалізовує увесь необхідний функціонал, по кожному з процесів забезпечення інформаційної безпеки. В процесі здійснення даного концептуального принципу необхідно звернути увагу, на те, що реалізація даного методу управління не повинна переслідувати за собою цілі заміщень\поєднань функцій засобів захисту інформації, а повинна лише управляти ними, що може бути досягнуто за допомогою інтеграції засобів захисту інформації і механізмів налаштування і управління ними у систему управління інформаційною безпекою.

Під принципом безперервності моделі управління інформаційною безпекою передбачається, що при реалізації цієї моделі необхідно забезпечувати безперервний цілеспрямований процес, що припускає здійснення контролю стану і управління усіма компонентами системи захисту інформації і вжиття відповідних заходів у випадку порушення працездатності на усіх етапах життєвого циклу системи захисту інформації починаючи з самих ранніх стадій проектування і модернізації, а також в процесі її експлуатації. При реалізації цього концептуального принципу необхідно обернути увага на необхідність збору і накопичення оброблюваних даних за системою захисту інформації в цілому і її окремим компонентам, з метою підтримки працездатності і своєчасного внесення змін. Більшості програмних і технічних засобів контролю і управління, включаючи реалізації цієї моделі, для ефективного виконання своїх функцій потрібна постійна організаційна (адміністративна) підтримка (своєчасна зміна і забезпечення пра-

вильного зберігання і застосування імен, паролів, ключів шифрування, перевизначення повноважень і тому подібне). Перерви в роботі цих засобів повинні зводитися до мінімального часу відновлення їх працездатності, що повинно бути закріплено на адміністративному рівні організації.

Під принципом спадкоємності і безперервності вдосконалення передбачається постійне вдосконалення заходів і засобів контролю і управління на основі спадкоємності організаційних і технічних рішень, кадрового складу, аналізу функціонування системи управління інформаційною безпекою і системи захисту інформації з обліком змін в методах і програмно-технічних засобах, нормативних вимог, в тому числі по захисту, накопиченого вітчизняного і зарубіжного досвіду в цій області. У процесі реалізації даного концептуально принципу необхідно приділити особливу увагу формуванню універсальних алгоритмів взаємодії даних при побудові системи управління інформаційною безпекою.

Під принципом розумної достатності передбачається економічна доцільність і порівнянність можливого збитку і витрат. Він припускає відповідність рівня витрат на використовувані заходи і засобів управління і контролю механізмів захисту інформації, що забезпечують інформаційну безпеку, цінності активів, що захищаються і величині можливого збитку від їх розголошування, втрати, витоку, знищення і спотворення. При реалізації цього концептуального принципу слід враховувати, що використовувані заходи і засоби реалізації цього методу не повинні помітно погіршувати основні характеристики системи захисту інформації.

Під принципом персональної відповідальності передбачається покладання

персональній відповідальності за управління і контроль засобами захисту інформації, що входять до складу системи захисту інформації, на кожного співробітника в межах його повноважень. Відповідно до цього принципу розподіл прав і обов'язків співробітників будується так, щоб у разі будь-якого порушення круг винуватців був чітко відомий чи зведений до мінімуму. В процесі реалізації цього концептуального принципу необхідно враховувати, що процеси розмежування прав доступу до інформації і засобів захисту інформації є однією з основ

методу управління інформаційною безпекою. Під принципом мінімізації повноважень передбачається надання користувачам і обслуговуючому персоналу, при реалізації методу, мінімальних прав доступу відповідно до виробничої необхідності. При реалізації даного концептуального принципу слід надавати доступ до механізмів управління інформаційною безпекою і інформації, що обробляється усередині, тільки у тому разі якщо це необхідно співробітникові для виконання його посадових обов'язків.

Під принципом наукової обгрунтованості і технічної, що реалізовується передбачається що інформаційні технології, технічні і програмні засоби, засоби і заходи управління і контролю методу управління інформаційною безпекою мають бути реалізовані на сучасному рівні розвитку науки і техніки, науково обгрунтовані з точки зору досягнення заданого рівня безпеки інформації і повинні відповідати встановленим нормам і вимогам по безпеці інформації, вживаним в організації.

Під принципом обов'язковості контролю передбачається обов'язковість і своєчасність виявлення і припинення спроб порушення встановлених регламентів роботи. Контроль за діяльністю користувачів і обслуговуючого персоналу системи управління інформаційною безпекою і системи захисту інформації і у відношенні будь-якого об'єкту захисту повинен здійснюватися на основі застосування засобів оперативного контролю і реєстрації і повинен охоплювати як несанкціоновані, так і санкціоновані дії користувачів і обслуговуючого персоналу. При реалізації цього концептуального принципу слід звернути особливу увагу, що повні механізми процесів аудиту в цей принцип не входять, а зачіпають лише його складові частини.

1.4 Огляд інструментальних засобів управління ризиками

Одним з найважливіших процесів в забезпечені інформаційної безпеку є оцінка ризиків небезпеки загроз. При роботі з ризиками спеціалісти стикаються з дуже великим об'ємом вхідної інформації. Тому є нагальна потреба в оптимізації такої роботи. Для ефективного забезпечення інформаційної безпеки використовують інструментальні засоби управління ризиками. Це такі продукти, як COBRA, CRAMM, Calleo Secura, OCTAVE, Risk Watch, vsRisk, Авангард та інші.

COBRA – набір програмних продуктів, які можна віднести до найпростіших засобів оцінки. В основному використовується для геп-аналізу (аналіз на відповідність ISO 27002). Інтерфейс застарілий. Оцінка ризику- якісна. Має досить високу вартість.

CRAMM – широко використовується у світі. Має широкий інструментарій, який включає базу знань, механізм мінімізації ризиків, засоби збору інформації, формує звіти, розраховує ризики. Оцінка ризику – кількісна та якісна. Користувач може додавати свої контрзаходи. Інтерфейс не зручний. Вартість продукта середня. Але недоліком є те, що продукт потребує спеціаліста високої підготовки і продукує багато паперової документації.

Calleo Secura є програмним продуктом для розробки, впровадження, експлуатації та сертифікації системи управління інформаційною безпекою Система надає допомогу в розумінні стандарту і приведення СУІБ у відповідність стандарту. Формує план створення СУІБ і має шаблони політик безпек. Оцінка ризику – якісна та кількісна. Потребує спеціальної підготовки спеціаліста. Система об'єднує функції управління ризиками з функціями управляння документами, контроль відповідності стандарту, передсертифікаційний аудит.

OCTAVE широко використовується, як метод для оцінки ризиків. Має зручний інтерфейс, не потребує спеціальної підготовки. Існує 3 методології: для ве-

ликих підприємств, для малих підприємств та для консультантів. Використовується якісна оцінка ризику. Не має можливостей визначати ризики для широкого кола ІТС, не можна задавати свої контрзаходи.

Risk Watch має ефективну, але досить складну методологію оцінки ризиків – кількісну. Програмний продукт має широка база знань по загрозам, вразливостям та контрзаходам. Є можливість редагування бази знань, можливість налаштування звітів. Потребує спеціальної підготовки. Інтерфейс не зручний.

vsRisk є новим сучасним засобом оцінки ризиків. Має простий та зрозумілий інтерфейс. Має інтегровану, регулярно оновлювану базу знань по загрозам та вразливостям. Оцінка ризику – якісна. Але має недоліки у вигляді проблем з відображенням кирилиці, загрози не пов'язані з активами, неможливо побудувати модель активів. Не надає пояснень вибору тих чи інших значень.

Авангард це комплексна експертна система управління інформаційною безпекою призначена для вирішення проблем управління безпекою у великих розподілених автоматизованих інформаційних системах, і призначена для полегшення контролю за центральними структурами рівня інформаційної безпеки на місцях. Цей комплекс є одним з найпотужніших інструментів для аналізу ризиків та контролю виробництва. Основні особливості системи: гнучка система введення та редагування моделі підприємства, можливість побудови моделі ризику, система оцінки ризиків та порівняння ризиків, оцінка контрзаходів, побудова варіантів заходів захисту та оцінка залишкового ризику.

Недоліки, які притаманні багатьом програмним продуктам для управління ризиками обмежують їх використання. До таких недоліків можна віднести: неповну відповідність міжнародним стандартам; неповне охоплення активів (ігноруються активи, які не відносяться до ІТ-активів); трудність в використанні; розрахунок ризику прихований від користувача.

Деякі відомі продукти не дозволяють проводити повноцінну оцінку ризиків (COBRA), а скоріше є засобами для аналізу невідповідності вимогам стандарту ISO 27001. Інші продукти (Calleo Secura) мають дуже слабкі засоби оцінки

ризиків та не повністю відповідають стандарту ISO 27001, зате мають інший потужній функціонал. А деякі продукти дуже складні в використанні та мають велику вартість (CRAMM).

Висновки до розділу 1

Таким чином, проаналізувавши національне та міжнародне законодавство в сфері управління інформаційною безпекою, можна зробити такі висновки:

1. Законодавство України охоплює практично всю область застосування СУІБ
2. Національне законодавство гармонізовано з міжнародним і постійно розвивається.
3. Держава надала всі інструменти для впровадження СУІБ в установах та на підприємствах

Проаналізувавши стандарти СУІБ, які представлені в Україні можна зробити такі висновки:

1. Сертифікація СУІБ по національним або міжнародним стандартам дозволяє підвищити ступінь привабливості організації на внутрішньому або зовнішньому ринках.
2. Стандарт COBIT марний для малих і в більшості випадків для середніх компаній. Він включає в себе дуже велику кількість абстрактної інформації та не відповідає на питання «як зробити». Тому підприємства з невеликим бюджетом для СУІБ навряд чи забажають впроваджувати саме його
3. Стандарт ITIL (IT Infrastructure Library) можна описати як приклад належної практики і рекомендацій для адміністрування IT-сервісами з фокусом на адмініструванні процесами. У той час як COBITS працює в питаннях управління та стандартизації підприємства, ITIL сконцентрований на процесах. Тобто COBIT визначає «ЩО», а ITIL - «ЯК». Але цей стандарт також не призначений для підприємств з невеликим бюджетом.

4. Стандарт, опублікований міжнародною організацією по сертифікації ISO та Міжнародної електротехнічної комісією IEC, виступає в якості відправної точки для групи стандартів, що забезпечують основи управління IT-безпекою, які можуть використовуватися будь-яким типом організацій (некомерційні, державні, приватні, великі чи маленькі). Тобто Стандарт ISO серії ISI 27 призначений конкретно для впровадження СУІБ і може застосовуватися на підприємстві середнього бізнесу.

Існуючі програмні засоби оцінки ризиків мають певні недоліки, тому при розробці експертної системи потрібно передбачити ці недоліки в частині повної відповідності стандарту ISO 27001, законодавству України та в тестуванні всіх активів підприємства на відповідність безпеці.

РОЗДІЛ 2. ПОБУДОВА СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВІ СЕРЕДНЬОГО БІЗНЕСУ

2.1. Процес побудови системи управління інформаційної безпеки

Процес побудови системи управління інформаційної безпеки носить комплексний характер і охоплює законотворчий, адміністративний, процедурний, програмно-технічний рівні. Різноманіття інформаційних систем породжує необхідність створення різних методик захисту інформації, що враховує індивідуальні особливості кожної системи. Сучасні ІС уразливі до низки мережних загроз, які можуть бути результатом реалізації несанкціонованого доступу, а також розкриття, викривлення або модифікації інформації. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи управління безпекою. Під управлінням інформаційною безпекою будемо розуміти циклічний процес, що включає: постановку задачі захисту інформації; збір та аналіз даних про стан інформаційної безпеки в ІС; оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію і впровадження відповідних механізмів контролю; розподіл ролей і відповідальності; політику безпеки; навчання та мотивацію персоналу, оперативну роботу зі здійснення захисних заходів; моніторинг (аудит) функціонування механізмів контролю, оцінку їх ефективності та надійності.

Процес впровадження системи управління інформаційною безпекою включає оцінку поточного стану інформаційного забезпечення захисту інформації ІКСМ, формування комплексу заходів щодо забезпечення оптимального рівня на основі оцінки ризиків. Після ідентифікації вимог безпеки варто вибирати й застосовувати заходи управління таким чином, щоб забезпечувати впевненість у зменшенні ризиків від реалізації несанкціонованого доступу. система управління

інформаційною безпекою – це «частина загальної системи управління організації, яка заснована на оцінці ризиків, створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення загальної інформаційної безпеки». Система менеджменту інформаційної безпеки – це та частина загальної системи менеджменту компанії, яка заснована на підході аналізу та оцінки бізнес-ризиків при створенні, впровадженні, функціонуванні, моніторингу, підтримці та покращенні інформаційної безпеки [31]. Цим документом прийнята циклічна модель PDCA [32]:

- Планування (Plan) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (Дія) – етап реалізації та впровадження відповідних заходів;
- Check (Перевірка) – фаза оцінки ефективності (аудит) та продуктивності СУІБ;
- Act (Покращення) – виконання превентивних та коригуючих дій.

Система менеджменту інформаційної безпеки розробляється з метою забезпечення вибору ефективних засобів управління безпекою, які призначені для захисту інформаційних активів. Вона об’єднує всі організаційні заходи в єдиний керований комплекс співставний реальним небезпекам та дозволяє досягати корпоративних цілей інформаційної безпеки [31].

Побудова СУІБ дозволяє чітко визначити, як взаємопов’язані процеси і підсистеми ІБ, хто за них відповідає, які фінансові і трудові ресурси необхідні для їх ефективного функціонування, і т. д.

Етапи створення СУІБ. Весь процес створення поділяється на декілька основних етапів:

1. Затвердження рішення про створення СУІБ.
2. Попередня підготовка.
3. Аналіз ризиків.
4. Розробка політик і процедур СУІБ
5. Впровадження СУІБ в експлуатацію [31].

Етап 1. Затвердження рішення про створення СУІБ. Рішення про створення СУІБ повинно прийматися керівниками компанії. Відділ захисту інформації (служба інформаційної безпеки) реалізовує початок даного процесу. У разі вирішення прийняття системи менеджменту інформаційної безпеки керівництво повинно усвідомлювати кінцеву ціль даного заходу та важливість сертифікації для бізнесу[30, 31].

Етап 2. Попередня підготовка. Наступним етапом є створення робочої групи та призначення керівника. До її складу мають увійти: представники керівництва організації, представники відділів, старші спеціалісти, що забезпечують інформаційну безпеку в компанії. Дані співробітники повинні усвідомленні про механізми систем менеджменту. До складу робочої групи можуть входити також консультанти, що спеціалізуються на питаннях СУІБ. Робоча група повинна мати всю необхідну нормативно-методичну базу для успішного створення, відповідно вимогам [30, 31].

Попередній аналіз оцінює галузі діяльності організації, які будуть охоплені СУІБ. При виборі області діяльності, в якій робоча група буде впроваджувати механізми СУІБ, повинні враховуватися наступні критерії: діяльність та послуги, що надаються організацією своїм партнерам і клієнтам, цільова інформація, безпека якої повинна бути забезпечена, бізнес - процеси, що забезпечують обробку інформації, відділи і співробітники організації, задіяні в даних бізнес – процесах, програмно - технічні засоби, що забезпечують функціонування даних процесів, територія компанії, в рамках яких відбуваються збір, обробка та передача інформації. Результатом є узгоджена та затверджена з керівництвом область діяльності організації, в рамках якої планується створення СУІБ[30, 31].

Також в процесі створення системи потрібно постійно аналізувати та виявляти невідповідності до нормативних документів. Для уточнення обсягу робіт і необхідних витрат на створення і подальшу сертифікацію СУІБ, члени робочої групи проводять роботи з виявлення й аналізу невідповідностей існуючих в організації заходів захисту до вимог стандарту. При цьому аналізуються як прий-

нятті організаційні заходи по плануванню, впровадженню, аудиту та модернізації, так і використовувані програмно - технічні засоби і механізми захисту інформації. На даному етапі компанія також може вибрати незалежний орган з сертифікації систем менеджменту, що має відповідну акредитацію. [31].

Етап 3. Аналіз ризиків. Найбільш складним завданням, що вирішуються в процесі створення СУІБ, слід назвати проведення аналізу ризиків інформаційної безпеки щодо активів організації в обраній галузі діяльності та прийняття керівництвом рішення про вибір заходів для зменшення ризиків

У процесі аналізу ризиків проводяться наступні роботи: ідентифікація всіх активів в рамках обраної діяльності, визначення цінності активів, ідентифікація загроз і вразливостей для даних активів, оцінка ризиків для можливих випадків успішної реалізації загроз, вибір критеріїв прийняття ризиків, підготовка плану оброблення ризиків[30, 31].

Виконання всіх зазначених завдань зазвичай здійснюється відповідно до розроблюваної процедурою аналізу ризиків, в якій визначена методологія і відображені організаційні аспекти.

Важливою ланкою аналізу ризиків є ідентифікація та визначення цінності активів. У рамках даних робіт повинні бути розглянуті всі бізнес - процеси, що входять в обрану область діяльності організації. По кожному бізнес - процесу, проводиться ідентифікація активів, а саме: інформаційні вхідні дані, вихідні дані, оброблювальні данні, працівники обраної галузі, інфраструктура, обладнання, програмне забезпечення.

Наступним кроком у проведенні аналізу ризиків, щодо активів компанії є визначення цінності активу, яка виражається у величині збитку для організації. Інформація про цінності активу може бути отримана від його власника або ж від особи, якій власник надав всі повноваження з даного активу. Результатом даних робіт є звіт про ідентифікацію та оцінку цінності активів .

Власне аналіз ризиків – це основний періодичний процес СУІБ. Необхідно підібрати таку методику аналізу ризиків, яку можна було б використати з міні-

мальними затратами часу та ресурсів. Можна використовувати існуючу чи розробити власну методику, яка найкращим чином підходитиме до специфіки компанії.

У процесі аналізу ризиків для кожного з активів або групи активів проводиться ідентифікація можливих загроз і вразливостей, оцінюється ймовірність реалізації кожної загрози і, з урахуванням величини можливого збитку для активу, визначається величина ризику, що відображає критичність загрози. В процедурі аналізу ризиків повинні бути ідентифіковані критерії прийняття ризиків та допустимі рівні ризику. Ці критерії мають базуватися на стратегічних, організаційних та управлінських цілях організації.

Керівники компанії використовують дані критерії, приймаючи рішення щодо прийняття контрзаходів для протидії виявленим ризикам. Якщо виявлений ризик не перевищує встановленого рівня, він є прийнятним, і подальші заходи по його обробці не проводяться. У випадку, якщо виявлений ризик перевищує прийнятний рівень, повинне бути прийняте одне з рішень: зниження ризику до прийнятного рівня за допомогою застосування відповідних контрзаходів; прийняття ризику; уникнення ризику; передача ризику[30, 31].

Після ідентифікації та опису можливих ризиків слідує під етап – «План обробки ризиків». Створюваний на даному етапі документ містить перелік першочергових заходів щодо зниження рівнів ризиків, а також цілі та засоби управління, спрямовані на зниження ризиків, із зазначенням: осіб, відповідальних за реалізацію даних заходів, термінів реалізації та пріоритетів їх виконання, ресурсів, рівнів залишкових ризиків. Прийняття плану обробки ризиків та контроль за його виконанням здійснює керівництво організації.

Виконання ключових заходів плану є відправною точкою для прийняття рішення про введення СУІБ в експлуатацію. [31].

Етап 4. Розробка політик і процедур СУІБ. Розробка організаційно – нормативної бази, необхідної для функціонування СУІБ, може проводитися паралельно з реалізацією заходів плану обробки ризиків. [31].

На даному етапі розробляються документи СУІБ. Зазвичай сюди входять такі політики та процедури: область діяльності, політика СУІБ. Також відносяться механізми забезпечення ІБ, такі як: політика антивірусного захисту; політика надання доступу до інформаційних ресурсів; політика використання засобів криптографічного захисту, тощо. Процедури ж можуть містити такі наступні заходи: управління документацією, управління записами, внутрішні аудити, коригувальні дії, попереджуючі дії, управління інцидентами, аналіз функціонування СУІБ керівництвом організації, оцінка ефективності механізмів управління СУІБ, інші процедури та інструкції. [31]..

Розроблені політики та процедури повинні охоплювати наступні ключові процеси СУІБ: управління ризиками, управління інцидентами, управління ефективністю системи, управління персоналом, управління документацією та записами системи управління ІБ, перегляд і модернізація системи, управління безперервністю бізнесу і відновлення після переривань. Крім того, в посадові інструкції відповідального персоналу, положення про підрозділи , контрактні зобов'язання організації повинні бути включені обов'язки щодо забезпечення інформаційної безпеки. Обов'язки з виконання вимог СУІБ за допомогою відповідних наказів та розпоряджень покладаються на відповідальних співробітників відділів. Всі розроблені положення політики, процедури та інструкцій доводяться до відома рядових співробітників при їх навчанні та інформуванні[30, 31].

Таким чином, в результаті не тільки створюється документальна база СУІБ, але й відбувається реальний розподіл обов'язків щодо забезпечення безпеки інформації серед персоналу[31].

Етап 5. Впровадження СУІБ в експлуатацію. Датою введення СУІБ в експлуатацію є дата затвердження компанії положення про внутрішній регламент обробки інформації . Даний документ є публічним і декларує цілі та засоби, обрані організацією для управління ризиками. Положення включає наступне: засоби управління і контролю, вибрані на етапі обробки ризиків, існуючі в організації засоби управління, засоби, що забезпечують виконання вимог законодавства, засоби, що забезпечують виконання загально корпоративних вимог, тощо.

При введенні СУІБ в експлуатацію використовуються всі розроблені механізми, що реалізують обрані цілі [30,31].

2.1.1 Рішення про створення СУІБ

Рішення розпочати програму створення СУІБ на підприємстві було запропоновано джира-адміністратором підприємства Чечугою Артемом, після чого генеральний директор схвалив це рішення. Згідно з наказом Генерального директора керівництво впровадження та функціонування СУІБ здійснює керівник відділу безпеки у зв'язці з відділом джира-адміністраторів. Для оперативного управління СУІБ в межах відділу безпеки створено підрозділ з питань інформаційної безпеки. Згідно з Наказом, керівники підрозділів – власників бізнес-процесів/комерційних продуктів мають сприяти впровадженню і функціонуванню СУІБ та своєчасно надавати необхідну інформацію керівникові СУІБ або його заступнику.

Для впровадження та подальшого вдосконалення СУІБ визначено вимоги з інформаційної безпеки підприємства джерелами вимог з інформаційної безпеки є:

- ISO/IEC 27001:2018;
- ДСТУ ISO/IEC 27001:2015;
- вимоги банків та систем переказу коштів;
- умови угод та договорів з третіми сторонами тощо.

2.1.2 Опис існуючої інфраструктури підприємства

Підприємство ТОВ «NDA» розроблює веб-сайти у навчальній сфері та розроблює своє ПО для SEO-аналізу.

Організаційно-правова форма підприємства – товариство з обмеженою відповідальністю з приватною формою власності.

Діяльність організації пов'язана з взаємодією з юридичними і фізичними особами на основі договору на купівлю реклами, трафіку, оренду серверів. ТОВ «NDA» має справу з комерційною таємницею, персональними даними та іншою конфіденційною інформацією. Вищий гриф секретності визначений як – «конфіденційно».

Територіально підприємство знаходиться у м.Києві. Підприємство знаходиться у 8-ми поверховій офісній-будівли, а саме на 7-8 поверхах.(Додаток А)

Захищеними приміщеннями є кабінет керівника і серверна. Підприємство функціонує 5 днів на тиждень. Графік роботи з 8:00 до 22:00.

Підприємство складається з наступних структурних підрозділів:

- генеральний директор;
- секретар генерального директора;
- Маркетинговий директор(Директор SEO-направлення: Seo-відділ);
- Технічний директор (Тімлід сис.адмінів: команда сис.адмінів), (Команда Jira-адміністраторів), (Тімлід команди розробки: команда розробки, команда тестувальників, команда проектних менеджерів, команда дизайнерів);
- Продукт менеджер (Команда розробки, команда тестувальників);
- Фінансовий директор; (Відділ бухгалтерського обліку, відділ фін.контролю, юридичний відділ);
- Адміністративний директор (Відділ охорони, клінінгова команда, офіс-менеджери);
- Директор відділу кадрів (Відділ рекрутингу, pr-підрозділ, hr-підрозділ);
- Продуктовий директор (Тімлід DS: команда обробки данних), (Тімлід Support: Команда підтримки), (Менеджер направлення: тімлід команди: проектний менеджер, дев-опс, тімлід розробки: команда розробки, тімлід тестувальників: команда тестувальників).

Організаційна структура ТОВ «NDA» класифікується, як лінійно-функціональна. Відповідно з такою структурою кожен співробітник організації підпорядковується керівництву свого функціонального блоку, а керівники відділів і команд - генеральному директору.(Рис. 2.2.).

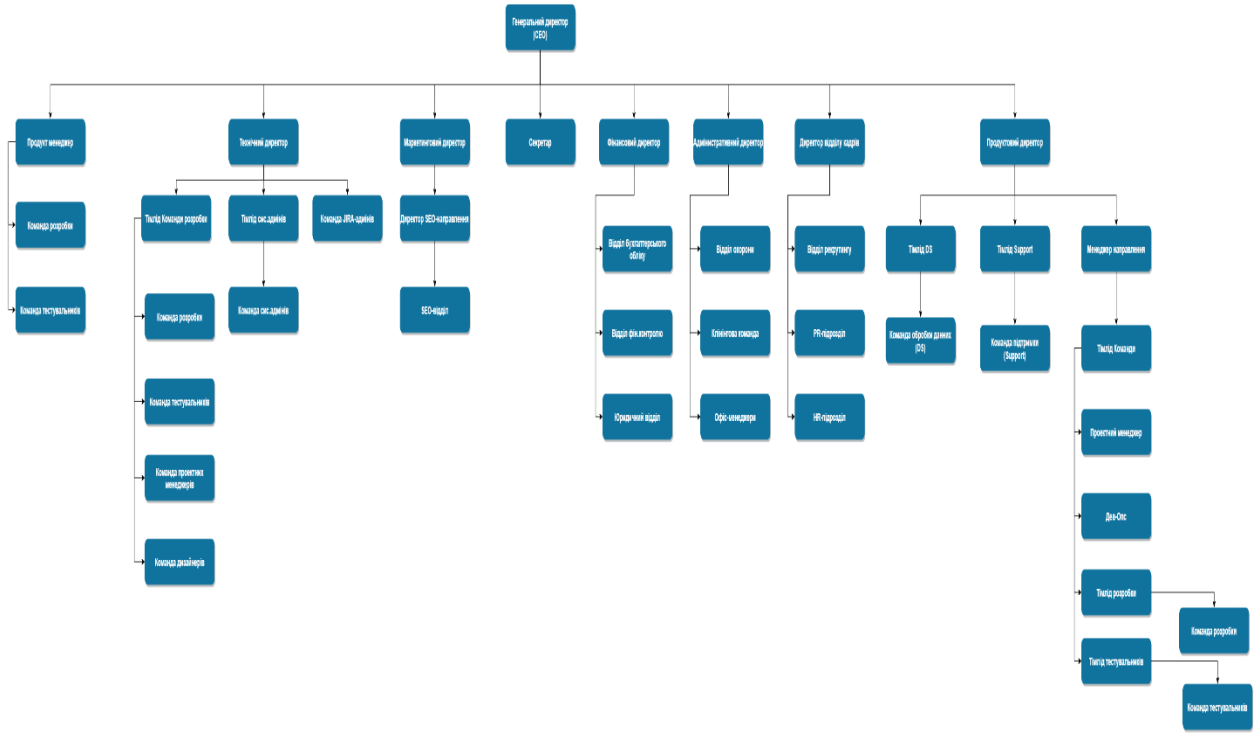

Рис.2.1. - Організаційна структура підприємства.

Опис існуючої інфраструктури було проведено для того, щоб визначити межі застосування СУІБ. Тому дуже важливо чітко визначити бізнес-процеси, організаційні одиниці, бізнес-підрозділи, інформаційні системи та інші складові підприємства, які працюють з інформацією з обмеженим доступом і повинні бути захищеними.

2.1.3 Етапи ідентифікації інформаційних активів

На сьогоднішній день інформаційна безпека – це 80 % менеджменту та 20 % технології. Під час реалізації першим та головним завданням є опис інформаційних активів організації [5]. При створенні методики опису інформаційних ак-

тивів використано процесний підхід та модель «Plan-Do-Check-Act» (цикл Шухарта-Деминга), тобто реалізується безперервне поліпшення процесу інформаційної безпеки організації [32].

Об’єктом СМІБ є інформаційні активи, тобто матеріальні або нематеріальні об’єкти, які є інформацією, або містять інформацію, або необхідні для оброблення інформації. Інформаційні активи володіють основними властивостями фінансових і матеріальних активів підприємства. Загалом цінність інформаційних активів набагато більша за фінансові активи підприємства [32].

Межі СУІБ включають організаційні одиниці, бізнес-підрозділи, інформаційні системи та інші складові підприємства. Таким чином, інвентаризація активів проводилась по всім бізнес-одиницям підприємства. Процес інвентаризації включив у себе:

- ідентифікацію бізнес-процесів;
- ідентифікацію інформаційних активів;
- ідентифікація власників активів;
- ідентифікацію фізичних та інформаційних ресурсів;
- визначення місць зберігання інформаційних активів.

2.1.4 Визначення бізнес-процесів підприємства

Всі бізнес-процесів визначались через відповідні структурні відділи підприємства, в рамках яких вони циркулюють. Розглядаються такі структурні підрозділи:

- Генеральний директор;
- Операційний департамент (відділ фін.контролю, юридичний відділ, відділ бухгалтерського обліку (+ директор));
- Відділ кадрів (відділ рекрутингу, hr-відділ, pr-відділ (+ директор));
- Адміністративний відділ (відділ охорони, офіс-менеджер (+ директор));

• Продуктовий відділ (Команда обробки данних(+ Тімлід команди), команда підтримки(+ Тімлід команди), відділ розробки(+ Менеджер));

• SEO-відділ (+ директор(маркетинговий));

• Технічний відділ (Команда Jira-адміністраторів, команда системних адміністраторів, команда розробки (+ директор(технічний)));

• Продуктова команда (+ менеджер).

Інформація, яка є цінною для підприємства циркулює в кожному структурному підрозділу. Частина, як приклад, бізнес-процесів підприємства з використанням моделі «граф-розгалужене дерево» наведено на малюнку (Рис. 2.2.) (Додаток Б).

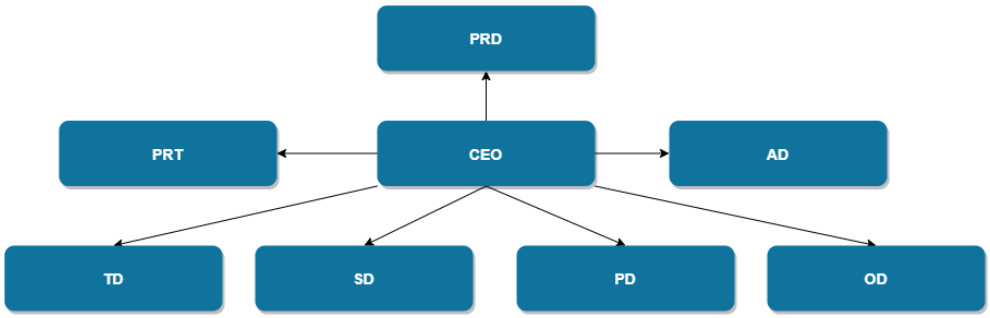

Рис. 2.2. – Розгалуження бізнец-процесів підприємства

AD – адміністративний департамент

AD – адміністративний директор.

CEO –головний директор.

CFO – фінансовий директор.

CMO – маркетинговий директор.

CTO – технічний директор.

DelM – делівері-менеджер

DEST – команда дизайнерів.

DevOps – девопс.

DEVT(0) – командра розробки (0)

DEVT(1) – команда розробників (1)

DevT(2) – команда розробки (2)

DevTL – тімлід розробки

DEVTL(0) – тімлід розробки (0).

DST – відділ обробки данних

DSTL – тімлід обробки данних.

FIN – фінансовий відділ.

HR – менеджер по роботі з людьми.

HRD – hr-директор.

HRR – рекрутингова команда.

JT – команда JIRA-адміністраторів.

LT – юридичний відділ.

OD – операційний департамент

OfM – офіс-менеджери

PD – відділ кадрів.

PE – бухгалтерський відділ.

PR – pr-команда

PRD - продуктовий департамент

PrM(2) – проджект-менеджер (2)

ProdD – продуктовий директор

ProjM – проджект-менеджер

ProjT – команда проджект-менеджерів

PRT – окрема продуктова команда.

QAT(0) – команда тестувальників (0)

QAT(1) – команда тестувальників (1)

QAT(2) – команда тестувальників 2()

QATL – тімлід тестувальників.

SD – SEO-департамент

SecD – відділ безпеки

ST – SEO-команда

SupT – команда підтримки.

SupTL – тімлід підтримки

SysD – системний відділ.

TD – технічний департамен

TLT – тімлід команди.

2.1.5 Визначення власників бізнес-процесів

Після ідентифікації всіх бізнес-процесів на підприємстві, було визначено всіх власників інформаційних активів. Як правило, це керівники бізнес-напрямків. Такі керівники мають повноваження і відповідальність для захисту важливої для бізнесу інформації. Власники бізнес-процесів є також власниками інформаційних активів, які створюються та / або використовуються в рамках їх напрямків діяльності. Власники бізнес-процесів повинні мати необхідні знання, щоб визначити критичність активу, і повинні мати повноваження, щоб організувати захист активу від порушення конфіденційності, цілісності та доступності. Обов'язки власника можуть бути делеговані, однак відповідальність повинна залишатися за призначеним власником активу (Додаток В).

2.1.6 Опис інформаційних активів

Згідно визначеної підприємством методики, було створено реєстр активів, тобто сформована таблиця в якій перераховані існуючі активи організації .

Опис активів відбувався за допомогою таких параметрів:

- назва активу;
- рівні забезпечення;
- носії інформаційного активу;
- власник активу;
- місце знаходження активу;
- категорія активу.

В таблиці виділено три рівні забезпечення: конфіденційність, цілісність, доступність.

Власником активу призначено особу, яка реально працює з активом і здатна впливати на властивості і стан активу.

Інформаційний актив – це будь яка інформація (відомість), яка представляє цінність для підприємства, його клієнтів, ділових партнерів та співробітників, а також будь-яка система для обробки інформації або фізичного місця її зберігання.

Для ідентифікації інформаційних активів проводилося інтерв'ю з кожним із визначених власників бізнес-процесів. В результаті опитування було визначено:

- яка інформація створюється і обробляється підрозділами в електронному та паперовому вигляді;
- фізичні місця, де інформація зберігається і обробляється, включаючи автоматизовані системи, файлові сервера, локальні комп'ютери, паперові документи, зовнішні місця зберігання (наприклад, системи контрагентів або постачальників) і фізичні локації;
- кожного користувача, який має доступ і працює з інформацією в або поза підприємством, із зазначенням посади, підрозділу (відділу);
- критичність інформації для підприємства;
- визначено рівні наслідків при порушені конфіденційності, цілісності та доступності (Таблиця 2.1)

Таблиця 2.1

Наслідки при порушенні КЦД

Рівень наслідків порушення КЦД	**Опис наслідків порушення**
4	Критичні наслідки, не зворотні (втрата частини ринку, закриття проектів, критичне зниження лояльності співробітників)
3	Дуже важливі наслідки, не зворотні (значні матеріальні втрати, отримання матеріальної вигоди конкурентами, Погіршення клімату в колективі)
2	Важливі наслідки, але зворотні (порушення приведуть до неправильної роботи інформаційних активів)
1	Значні наслідки, результати від яких проявляться через деякий час, без порушень в роботі
0	Незначні порушення (наслідки відсутні)

2.1.7 Перелік інформації, що обробляється на підприємстві

Інформація, що обробляється в АС є власністю даної фірми та її клієнтів. За режимом доступу інформація в АС має бути поділена на [32]:

- відкриту інформацію;
- інформацію з обмеженим доступом.

Проаналізувавши бізнес – процеси підприємства, було визначено, що в АС Підприємства обробляється відкрита та інформація з обмеженим доступом - конфіденційна інформація. До конфіденційної інформації відносяться дані, що пов'язані з персональними даними, технологічна та ключова інформація. Інформація загального користування є відкритою інформацією (Таблиця 2.2).

Таблиця 2.2

Інформація, що обробляється на підприємстві

Шифр	**Назва**	**Тип доступу**
{BDA}	Бази даних (всі)	Конфіденційна
{WSP}	Веб-сайти підприємства	Відкрита
{ZKB}	Записи з камер відеоспостереження	Відкрита
{IPVV}	Інформація з пристроїв введення	Відкрита
{IPV }	Інформація з пристроїв виведення	Відкрита
{UZ}	Управлінські звіти	Конфіденційна
{ISysPZ}	Інформація системне ПЗ	Конфіденційна
{IPrPZ}	Інформація прикладне ПЗ	Конфіденційна
{ISlPZ}	Інформація службове ПЗ	Конфіденційна
{ISpPZ }	Інформація спеціальне ПЗ	Конфіденційна

Користувачі мають різні повноваження стосовно доступу до інформації з обмеженим доступом, яка розміщується на носіях інформації.

На носіях інформації зберігаються дані різних ступенів обмеження доступу. Гриф обмеження доступу носія інформації відповідає вищому ступеню обмеження доступу даних, які на ньому зберігаються.

Документи, в яких містяться ІзОД, друкуються за допомогою принтера, який входить до складу АС ТЗІ.

Носії інформації з ІзОД знаходяться на обліку та зберігаються в відділі захисту інформації підприємства. Доступ до них регламентується розпорядчими документами цього підприємства.

Порядок копіювання файлів, стирання інформації, опрацювання документів здійснюється згідно вимог розпорядчих документів підприємства.

2.2. Оцінка та ідентифікація загроз інформаційній безпеці

Загрози циркулюючої в ІС інформації залежать в загальному випадку від структури і конфігурації ІС, технології обробки інформації в ній, стану навколишнього фізичного середовища, дій персоналу і структури самої інформації. Є різні способи класифікації загроз інформації, але найбільш загальною (базовою) є класифікація загроз за наслідками можливого впливу на інформацію [32]:

- загрози порушення конфіденційності;
- загрози порушення цілісності;
- загрози порушення доступності

На підприємстві інформаційні загрози класифіковані за характером, типом і способом їх реалізації. Загрози для інформації представлені у вигляді таблиці (Додаток Г).

2.2.1 Методика оцінки загроз на підприємстві

Існуючі на сьогоднішній день методи обліку та оцінки в галузі інформаційної безпеки дуже суб'єктивні і призводять до невірних оцінок ризиків. Теорія нечіткої логіки – це новий проект, який динамічно розвивається. Останнім часом нечітке моделювання є одним з найбільш активних і перспективних направлень прикладних досліджень в області управління ризиками і управління інформаційною безпекою. При оцінці загроз присутня невизначеність, яка ускладнює застосування точних кількісних методів і підходів. Тому методику оцінки ризиків побудуємо за допомогою теорії нечітких множин. Основною відмінністю методу є введення лінгвістичної змінної, а також кількісне значення факторів, які будуть впливати на лінгвістичну змінну.

Таким чином, оцінено загрози інформаційній безпеці використовувати теорію нечітких множин [33]. Задано лінгвістичну змінну (ЛЗ). Лінгвістична зміна приймає нечіткі значення (терм-значення):

$T = \{T_1, T_2, T_3, T_4, T_5\}$, де

T_1 – Не велика

T_2 - Велика

T_3 - Небезпечна

T_4 – Критична

T_5 – Дуже критична

Для визначення носія множини Ωt, який містить терм-значення Т проведено бальний метод експертної оцінки. На оцінку небезпеки загрози впливає ряд факторів, які приймають наступні значення:

P_1 – об'єкт загрози (1 – фізичні ресурси ; 2 – інформаційні ресурси; 3 – людські ресурси);

P_2 – джерело загрози (1 – природне; 2 – техногенне; 3- антропогенне.);

P_3 – розташування джерела загрози (1 - внутрішнє; 2 - зовнішнє);

P_4 - мета загрози (1 – порушення конфіденційності; 2 – порушення цілісності; 3 – порушення доступності);

P_5 - навмисність дій (1 – ненавмисне; 2 – навмисне);

P_6 - рівень порушника (1 - низький; 2 – середній; 3 – високий; 4 – дуже високий);

P_7 - можливість нейтралізації загрози (1 - легко; 2 – важко; 3 – дуже важко; 4 – неможливо);

P_8 – можливість виявлення загрози (1 - легко; 2 – важко; 3 – дуже важко; 4 – неможливо);

P_9 – можливість відновлення об'єкта після загрози (1 - легко; 2 – важко; 3 – дуже важко; 4 – неможливо);

P_{10} - частота появи загрози за рік (1 – невідомо; 2 - низька; 3 – середня; 4 – висока; 5 – дуже висока);

P_{11} – небезпека реалізації загрози стосовно збитку (1 – незначна; 2 - низька; 3 - середня; 4 – висока; 5 – критична);

P_{12} – витрати на реалізацію загрози (1 –незначні; 2 - середні; 3 - високі; 4 – дуже високі;);

P_{13} – простота реалізації загрози (1 – дуже важко; 2 - важко; 3 – відносно легко; 4 – легко).

Показники ступеню небезпеки загрози зведемо у таблицю (Таблиця 2.3) і розрахуємо інтервали для кожного терм-значення. Таким чином отримаємо оцінку носія множини небезпеки загрози (Ωt).

Таблиця 2.3

Показники ступеню небезпеки загрози

Показник		**Терм-значення**			
	T_1	**T_2**	**T_3**	**T_4**	**T_5**
P_1	1-3	1-3	1-3	1-3	1-3
P_2	1-3	1-3	1-3	1-3	1-3
P_3	1-2	1-2	1-2	1-2	1-2
P_4	1-3	1-3	1-3	1-3	1-3
P_5	1-2	1-2	1-2	1-2	1-2
P_6	1-2	1-2	1-3	2-4	3-4
P_7	1-1	1-2	1-3	2-3	3-4
P_8	1-1	1-2	1-3	2-3	3-4
P_9	1-1	1-2	2-3	3-4	3-4
P_{10}	1-2	1-2	2-3	2-4	3-4
P_{11}	1-2	1-2	2-3	3-4	3-4
P_{12}	1-2	1-2	2-3	3-4	3-4
P_{13}	1-2	1-2	2-3	3-4	3-4
	13-26	13-26	18-37	25-43	29-45

Таблиця 2.4

Експертна оцінка небезпеки загроз (в балах)

Загрози	**Показники небезпеки загроз**													
	P_1	**P_2**	**P_3**	**P_4**	**P_5**	**P_6**	**P_7**	**P_8**	**P_9**	**P_{10}**	**P_{11}**	**P_{12}**	**P_{13}**	**K_1**
Несанкціонований збір інформації.	2	3	1	3	2	3	1	3	1	1	1	4	2	27
Несанкціонований доступ	2	3	1	3	2	3	2	3	2	2	2	4	2	31
Мережеві загрози	2	3	1,2	2	1,2	3	2	1	3	4	4	3	4	37
Побічні явища	2	2,3	2	2	1,2	1	1	1	1	1	1	2	3	25
Відмови, помилки	1	2	1	3	1,2	1	3	1	2	3	3	3	2	28
Аварійні ситуації	1	2	1,2	2	1,2	1	4	1	2	4	2	3	4	32

Оціночні показники по кожному фактору відповідної загрози занесено в таблицю (Таблиця 2.4).

Кількісний показник небезпеки загроз розраховуємо по формулі:

$$k_1 = \sum_{i=1}^{n} P_i$$

Де,

K_1 - сума показників небезпеки загроз

P_i - показник небезпеки загроз

Функції належності і-ї небезпеки загрози одному із терм-значень $T_1T_2T_3T_4T_5$ зведено в таблицю (Таблиця 2.5).

Таблиця 2.5

Матриця оцінки небезпеки загроз підприємства

Загроза	**$K_1(t_i)$**	**Функції належності**				
		μ_{T_1}	**μ_{T_2}**	**μ_{T3}**	**μ_{T4}**	**μ_{T_5}**
Несанкціонований збір інформації.	27	0	0	0,5	0,1	0
Несанкціонований доступ	31	0	0	0,7	0,3	0,1
Мережеві загрози	37	0	0	0,9	0,7	0,6
Побічні явища	25	0,9	0,9	0,4	0,1	0
Відмови, помилки	28	0	0	0,5	0,2	0
Аварійні ситуації	32	0	0	0,7	0,5	0,2
		13-26	13-26	18-37	25-43	29-45

По даним наведеним у таблиці 2.5 побудуємо гістограму розподілу загроз по ступеню небезпеки (Рис. 2.3.)

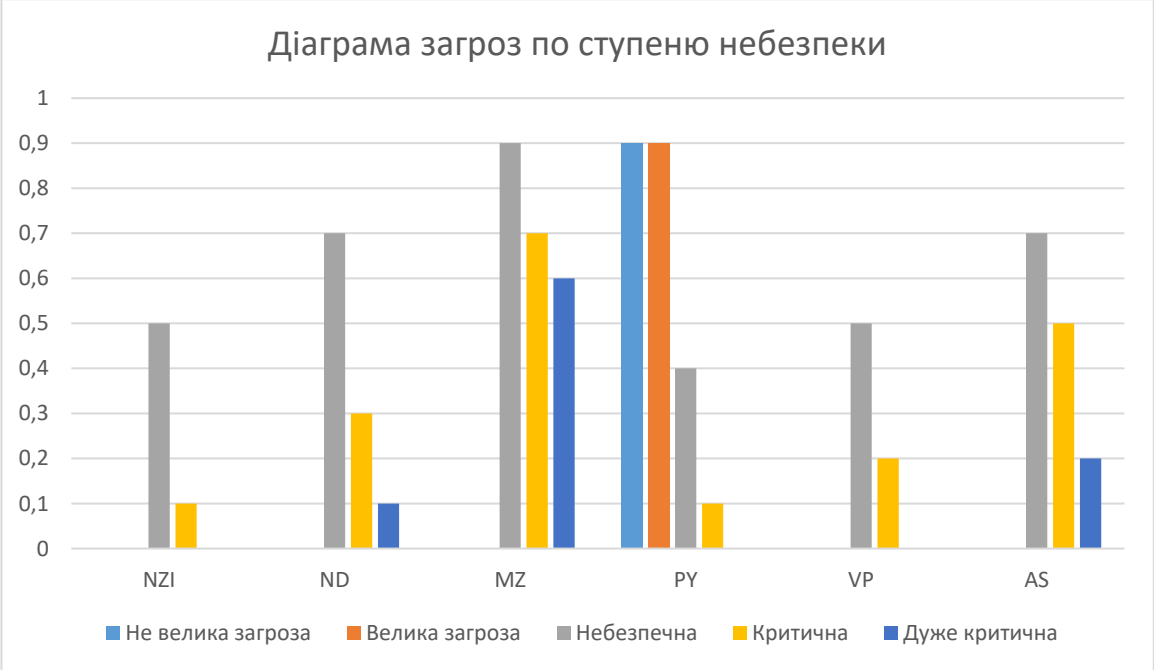

Рис. 2.3. - Діаграма загроз по ступеню небезпеки

Отримавши данні керівництво повинно звернути увагу, що мережеві загрози та побічні явища для підприємства є дуже небезпечними та критичними. Також аварійні ситуації є небезпечними з досить великою ймовірністю настання.

Отримавши такий високий бал критичності небезпеки загрози, керівництво повинно передбачити низку заходів по протидії реалізації цієї загрози.

2.2.2 Методика оцінки та ідентифікації інформаційних активів

Ідентифікація ресурсів потрібна для створення моделі захисту інформації і наступної оцінки важливості активу з точки зору захисту інформації.

Для оцінки важливості інформаційних активів також використовуємо теорію нечітких множин. Вводимо лінгвістичну змінну (ЛЗ). Лінгвістична зміна приймає нечіткі значення:

$A = \{A_1, A_2, A_3, A_4\}$, де

A_1 – Не важливий

A_2 - Важливий

A_3 - Критичний

A_4 – Дуже критичний

Проведемо бальний метод експертної оцінки для визначення носія множини Ωa, який містить вище наведені терм-значення А. Так як на оцінку активу впливають різні фактори, будемо використовувати наступні значення:

V_1 – загроза конфіденційності (1 – не велика, збиток малоймовірний; 2 - безпечна, інколи може бути невеликий збиток; 3 - небезпечна, незначні збитки; 4 – критична, значні збитки; 5 – дуже критично, неприпустимі збитки або крах роботи);

V_2 - загроза цілісності (1 – не велика, немає наслідків; 2 - безпечна, збою в роботі немає, наслідки можуть відбутися через деякий час; 3 - небезпечна, невірна робота активу, наслідки оборотні; 4 – критична, невірна робота активу, наслідки оборотні; 5 – дуже критично, неприпустима, невірна робота активу, наслідки необоротні);

V_3 – загроза доступності (1 – не велика; 2 - безпечна, працювати можливо, наслідки оборотні; 3 - небезпечна, працювати можливо, наслідки оборотні; 4 –

критична, працювати можливо короткий час, наслідки оборотні; 5 – дуже критична, робота зупиняється, наслідки необоротні).

V_4 – вартість активу первісна (1 - незначна; 2 - середня; 3 - значна; 4 – критична; 5 –дуже критична);

V_5 – вартість активу при частковому відновленні в результаті реалізації загрози (1 - незначна; 2 - середня; 3 - значна; 4 – критична; 5 – дуже критична);

V_6 - вартість активу при його повному відновленню в результаті реалізації загрози (1 - незначна; 2 - середня; 3 - значна; 4 – критична; 5 – дуже критична);

V_7 - час на відновлення активу при частковому руйнуванню в результаті реалізації загрози (1 -до І години; 2 – до 1 доби; 3 – від 1 до 6 діб; 4 – від 1 до 4 тижнів ; 5 – 1 місяць і більше);

V_8 - час на відновлення активу при повному руйнування в результаті реалізації загрози (1 - до 1 години; 2 – до 1 доби; 3 – від 1 до 6 діб; 4 – від 1 до 5 тижнів ; 4 – 1 місяць і більше);

V_9- відновлення втраченого активу в результаті реалізації загрози (1 – не важко; 2 – середня важкість, необхідні незначні часові, трудові або матеріальні витрати; 3 – важко, необхідні значні часові, трудові або матеріальні ресурси; 4 – критично, необхідні значні часові або недопустимі матеріальні витрати; 5 – дуже критично, відновлення неможливе)

V_{10} – важливість активу для всієї інформаційної системи, вплив на роботу інших активів (1 – не впливає; 2 – впливає, але небезпеки немає, збій може відобразитися на роботі інших активів через деякий час; 3 – впливає на незначну частину активів, небезпека середня; 4 – впливає критично, призводить до зупинки роботи більшої частини активів; 5 – критично, вся інформаційна система стає неробочою).

Оцінено кожний актив відповідно до факторів, які впливають на такий актив. Проведемо бальну оцінку і занесемо данні в таблицю (Таблиця 2.6). Тим самим буде визначено носій множини Ωa.

Таблиця 2.6

Таблиця оцінок носія множини Ωа

Показник	**Терм-значення**			
	A_1	**A_2**	**A_3**	**A_4**
V_1	1-2	2-3	3-4	4-5
V_2	1-2	2-3	3-4	4-5
V_3	1-2	2-3	3-4	4-5
V_4	1-2	1-2	2-3	3-4
V_5	1-2	1-2	2-3	3-4
V_6	1-2	2-3	3-4	4-5
V_7	1-2	1-2	2-3	3-4
V_8	1-2	2-3	3-4	4-5
V_9	1-2	2-3	3-4	3-5
V_{10}	1-2	1-3	2-4	3-5
	10-20	16-27	26-37	35-47

Як видно з Таблиці 2.6 носієм множини Ωа є відрізок [10:37].

По кожному інформаційному активу експерти виставляють бали та заносять їх в таблицю (Таблиця 2.7).

Таблиця 2.7

Оцінка важливості інформаційних активів підприємства

Актив	**Показники важливості активу**										
	V_1	**V_2**	**V_3**	**V_4**	**V_5**	**V_6**	**V_7**	**V_8**	**V_9**	**V_{10}**	**K_2**
Сервер загального призначення	2	4	4	4	4	4	4	4	4	4	38
База даних	4	4	4	4	3	4	4	4	4	4	39
База даних	4	4	4	4	3	4	4	4	4	4	39
Пристрій введення	1	3	4	2	2	1	1	1	1	4	20
Пристрій виведення	1	3	4	2	2	1	1	1	1	4	20
Файли	3	3	3	3	3	3	3	3	3	3	30
Паперові документи	4	4	4	4	4	4	3	4	3	4	38
Системне ПЗ	2	4	4	3	3	3	3	4	4	5	35
Прикладне ПЗ	2	4	4	2	2	2	2	3	3	2	26
Службове ПЗ	3	4	4	3	4	3	2	4	4	4	35
Спеціальне ПЗ	4	4	5	5	4	4	3	5	5	5	44

Кількісний показник важливості активу розраховується по формулі:

$$\mathbf{k_2} = \sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{V_i}$$

Де,

K_1 - сума показників важливості активу

V_i- показник важливості активу

Функції належності і-го активу одному із терм-значень $A_1A_2A_3A_4$ зводимо в таблицю (Таблиця 2.8)

Таблиця 2.8

Матриця оцінки активів підприємства

Актив	**$K_2(a_i)$**	**Функції належності**			
		μ_{a_1}	**μ_{a_2}**	**μ_{a_3}**	**μ_{a_4}**
Сервер загального призначення	38	0	0	0	0,2
База даних	39	0	0	0	0,3
Пристрій введення	20	0,9	0,4	0	0
Пристрій виведення	20	0,9	0,4	0	0
Файли	30	0	0	0,4	0
Паперові документи	38	0	0	0	0,2
Системне ПЗ	35	0	0	0,8	0,1
Прикладне ПЗ	26	0	0,9	0,1	0
Службове ПЗ	35	0	0	0,8	0,1
Спеціальне ПЗ	44	0	0	0	0,9

По отриманим даним, побудовано гістограму по рівню важливості інформаційних активів підприємства (Рис. 2.4.).

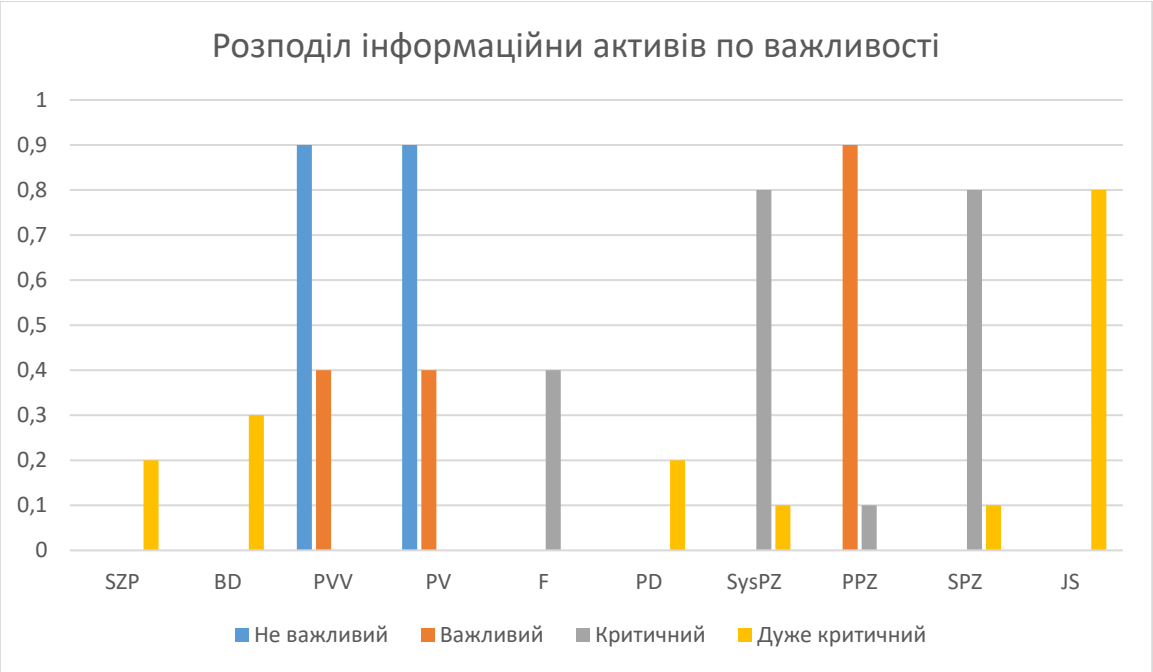

Рис. 2.4 - Гістограма розподілу інформаційних активів по ступеню важливості

Отримана оцінка дозволяє визначити критичність любого активу по всій системі інформаційної безпеки підприємства. Описана методика дозволяє додавати та оцінювати будь-який інформаційний ресурс в загальній системі захисту.

Отже, методика ідентифікації і оцінки інформаційного активу характеризує рівень важливості та вразливості інформаційного активу з точки зору інформаційної безпеки підприємства.

Так як кожен актив був описаний за допомогою різних факторів, які впливають на його важливість, то кожний актив можна проаналізувати на різні параметри важливі для безпеки. Наприклад, крім того, кожна графа в таблиці характеризує різні параметри важливі для безпеки. Так , наприклад, очевидно, що до ІА з рівнем важливості « Дуже критичний» відноситься спеціальне ПЗ - JS.

2.3 Розрахунок ризиків та рівня забезпечення інформаційної безпеки

2.3.1 Розрахунок та аналіз ризиків

Для побудови СУІБ необхідно провести повний аналіз ризиків з метою визначення можливих ризиків для інформаційних активів у разі реалізації таких загроз.

Збиток може настати в результаті реалізації загроз та залежить від показників цінності інформаційних активів, ймовірності реалізації загрози та вразливостей.

Оцінка ризиків заснована на використанні якісних величин оцінок загроз, активів та вразливостей (Таблиця 2.12). Вразливість активу визначається як низька (Н), середня (С), висока (В), а показники ризику належать інтервалу від 0 до 9 [10,11].

Таблиця 2.9

Значення ризиків для загроз, активів та вразливості інформаційної системи

Оцінка загрози	**Оцінка активу**											
	Не важливий			**Важливий**			**Критичний**			**Дуже критичний**		
	Н	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
Не велика	0	1	2	1	2	3	2	3	4	3	4	5
Велика	1	2	3	2	3	4	3	4	5	4	5	6
Небезпечна	2	3	4	3	4	5	4	5	6	5	6	7
Критична	3	4	5	4	5	6	5	6	7	6	7	8
Дуже критична	4	5	6	5	6	7	6	7	8	7	8	9

Величина ризику в показниках і шкалах даної методики належить інтервалу від 0 до 9:

0 - ризик відсутній;

1 - ризик практично відсутній. Теоретично можливі ситуації, при яких загроза буде реалізована, але на практиці це трапляється рідко, а потенційний збиток порівняно невеликий;

2 - ризик незначний. Реалізація загрози трапляється дуже рідко, негативні наслідки порівняно невеликі;

3 - ризик низький. Реалізація загрози трапляється іноді, наслідки незначні і легко усуваються. Збитком можна знехтувати;

4 - ризик помірний. Збиток від реалізації загроз можливо усунути, витрати на ліквідацію наслідків реалізацій загроз невеликі;

5 - ризик середній. Ліквідація наслідків реалізації загроз не пов'язана з великими витратами і не зачіпає критично важливі завдання, але становище на ринку погіршується, частина клієнтів може бути втрачена;

6 - ризик вище середнього. Ймовірність реалізації загроз середня, негативні наслідки можуть бути значущими, ліквідація наслідків потребує деяких зусиль. Ліквідація наслідків реалізації загрози пов'язана з фінансовими інвестиціями, організація залишається здатною частину функцій виконувати деякий час;

7 - ризик високий. Наслідки від реалізації загроз важкі, для ліквідації будуть потрібні значні часові та матеріальні витрати. Виконання важливих завдань стає важким. Втрата на деякий період положення на ринку;

8 - ризик дуже високий. Ускладнюється виконання критично важливих завдань. Втрата на тривалий період положення на ринку. Ліквідація наслідків реалізації загрози пов'язана зі значними фінансовими інвестиціями;

9 - ризик критичний. Наслідки реалізації загрози можуть бути катастрофічними для організації. Реалізація загрози призводить до неможливості вирішення критично важливих завдань. Організація припиняє існування.

Визначені ризики аналізуються і приймається рішення про допустиму величину ризику. Допустимою величиною ризику на підприємстві прийнято показник $R\_ac \leq 4$. Якщо величина ризику більше допустимої, то приймається декілька заходів протидії, які повинні бути адекватні виявленим ризикам

За результатами оцінки ризиків по кожній загрозі ІБ можуть бути прийняті наступні типи рішень:

- прийняття ризику - для тих загроз, ймовірність реалізації яких незначна, або збиток від реалізації якої вважається прийнятним. Критерії для відсіву таких ризиків визначаються в завданні на обробку ризиків. Загрози з таким ризиком не представлені в приватній моделі загроз і відсіяні на етапі обробки ризиків;

- зниження ризику - дії спрямовані на: виправлення, усунення, запобігання, мінімізацію впливу, стримування, виявлення, відновлення, контроль і розуміння ризику. Перелік загроз, ризик реалізації яких вимагає зниження, є осно-

вною частиною моделі загроз. Вимоги щодо зниження рівня ризику визначаються на підставі моделі загроз приватними політиками інформаційної безпеки та іншою документацією. Зниження ризику відбувається шляхом використання простих заходів. Наприклад, на підприємстві є дуже високий ризик несанкціонованого доступу практично до всіх активів, але розробка вимог до управління паролями та її впровадження знизить ризик НСД;

- ухилення від ризику – Рішення базується на том, що від деяких ризиків можна ухилитися, якщо побудувати комплексну модель захисту інформації починаючи з організаційних методів. Наприклад, якщо винести Web-сервер підприємства за межі локальної мережі, то це дозволить запобігти ризику НСД зі сторони Web-клієнтів. Також можливо фізично перенести місце обробки інформації в місце де ризик не існує або є під контролем. На підприємстві можливо підвищити рівень захищеності паперових документів, якщо впровадити на підприємстві вимоги до зберігання паперових документів і зберігати їх в відповідному приміщенні;

- перенесення ризику дозволяє розділити певні ризики з зовнішніми сторонами. Перенесення ризику може створити нові ризики або змінити існуючі ідентифіковані ризики. Тому може бути необхідною додаткова обробка ризику. Перенесення може бути за рахунок страхування, яке візьме на себе наслідки або, укласти договір з партнером, який буде тримати під контролем інформаційну систему і здійснить безпосередні дії, щоб зупинити атаку перш, ніж вона зробить певний рівень пошкоджень.

Так як на підприємстві ТОВ «NDA» прийнятий тип ризику перенесення, то підприємство делегує повноваження по охороні території сторонній організації, а також використовує страхування обладнання, включаючи сервера. Але це не повністю запобігає виникненню загроз інформації. На думку виконавця, потрібно використовувати додаткові заходи безпеки.

На підприємстві важливо підвищити рівень захищеності спецального ПЗ.

Висновки до розділу 2

У даному розділі було проведено опис структури підприємства, визначено бізнес-процеси, які наявні на підприємстві, визначено власників бізнес-активів компанії.

Також, розроблена методика забезпечення інформаційної безпеки підприємства, яка включає наступне:

- ідентифіковані та оцінені інформаційні активи та ймовірні загрози для таких активів;
- побудовано гістограму розподілу загроз по ступеню небезпеки;
- побудована гістограма розподілу інформаційних активів по ступеню важливості;
- визначені і оцінені значення ризики для загроз, активів та вразливості інформаційної системи.

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ІБ НА ПІДПРИЄМСТВІ

3.1. Огляд спеціального програмного забезпечення

Основним і найголовнішим інформаційним активом компанії є Jira.

Jira Software є частиною сімейства продуктів, розроблених з метою спрощення управління робочим процесом для різних команд. Спочатку Jira створювалася як система відстеження завдань і помилок. Але сьогодні Jira перетворилася на потужний інструмент управління роботою, що підходить для самих різних випадків, від управління вимогами та сценаріями тестування до agile-розробки програмного забезпечення. Прочитавши це , ви дізнаєтеся, які функціональні можливості Jira зможуть задовольнити унікальні потреби вашої команди.

Сьогодні все більше команд розробляють все більш ітеративно, і Jira Software є центральним вузлом на етапах кодування, спільної роботи і випуску.

Для управління тестуванням Jira інтегрується з безліччю налаштувань, тому тестування QA плавно переходить в цикл розробки програмного забезпечення.

Команди можуть проводити ефективне ітеративне тестування.

Команди QA використовують задачі Jira, налаштовані екрани, поля і робочі процеси для управління ручними і автоматичними тестами.

Для команд, які практикують гнучкі методології, Jira Software пропонує готові дошки скрам і канбан. Дошки - це центри управління задачами, де задачі зіставляються з налаштованим робочими процесами.

Можливості відстеження часу і звіти про продуктивність в реальному часі (графіки вигорань / спрінтів, звіти про спрінти, графіки швидкості) дозволяють командам уважно відслідковувати свою продуктивність з плином часу.

У Jira створені проекти, за кожним бізнес-процесом закріплено певний проект, проект створювався і налаштовувався залежачи від специфіки команди-процесу. В чому ж найголовніша суть? Справа в тому що, майже всі працівники компанії (окрім клінерів) використовують JIRA для своєї роботи, тобто вся інформація знаходиться саме там. Усі користувачі розмежовані по групах, саме за групами налаштована сек'юрність і доступність до проектів. У кожному проекті можна розгалужувати певні групи або окремих юзерів по ролях. Ролі проекту дозволяють асоціювати користувачів з певними функціями. Тобто за розробку відповідають одні, за адміністрування інші і т.д. Приклад продемонстровано на малюнку (Рис 3.1.)

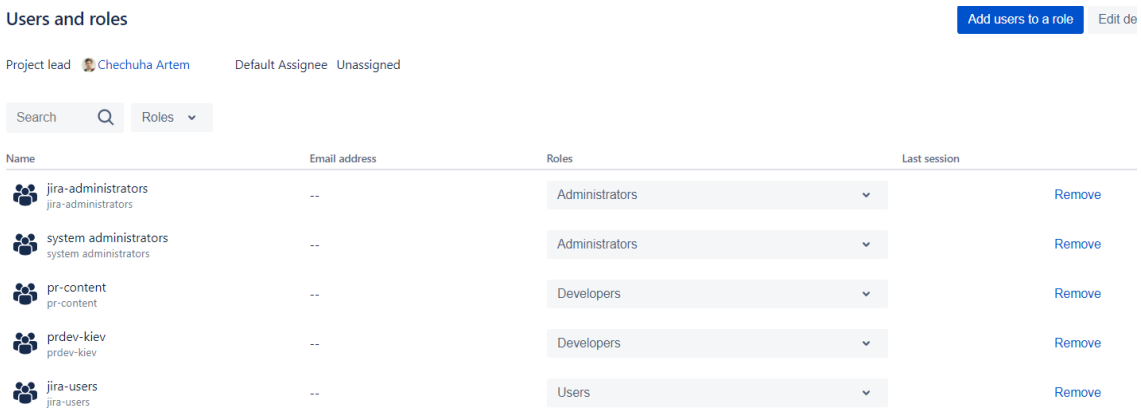

Рис. 3.1. – Приклад розмежування юзерів по ролям

Як працювати з Jira? Уся робота компанії ведеться у проектах через таски. Що ж таке таски? Таски або задачі - завдання, які створюють юзери на свій чи інший відділи. У кожному проекті кастомно налаштовані різні типи задачи, різні екрани для типів задач та пов'язані з ними поля. Наприклад, якщо нам потрібно, щоб для нас засетапили сайт, то потрібно ставити таск на системних адміністраторів у відповідний проект., заповнюючи усі обов'язкові поля, які є на екрані створення таску. Приклад створення таску показано на скріншоті (Рис. 3.2.)

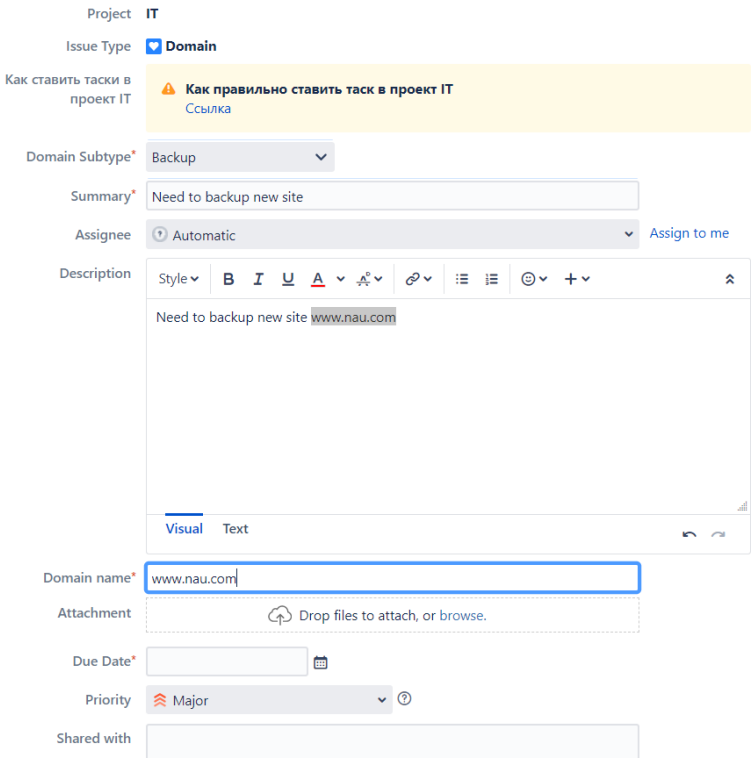

Рис. 3.2. – Створення таску

Після створення таску, задача падає на відповідну особу, яка спочатку перевіряє на корректність веддення всіх данних, а потім вирішує, чи потрібно брати задачу в роботу, чи ні.

Результат і приклад створеного таску можна побачити на рисунку (Рис. 3.3.)

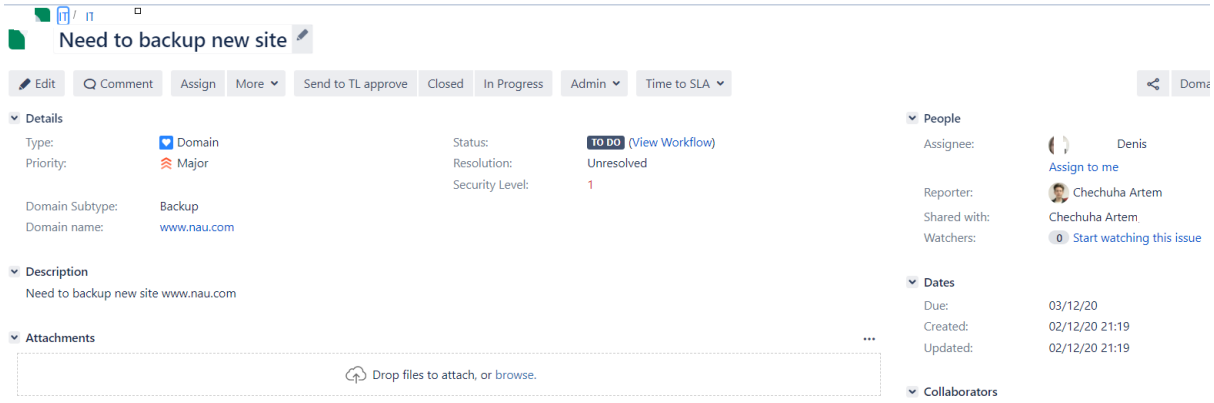

Рис. 3.3. – Створений таск

Робота за задачею ведеться по передчасно налаштованому робочому процесі, на переходах якого налаштована різна логіка: зміна відповідальних за задачею, зміна перевіряючих задачу, спеціальні умови та інше. Демонстрація робочого процесу представлена на малюнку (Рис. 3.4.)

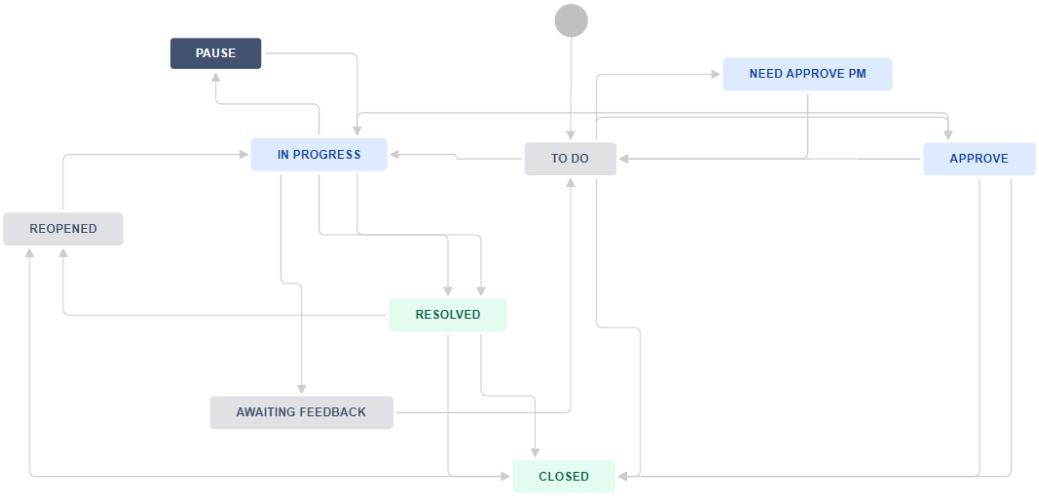

Рис. 3.4. - Робочий процес у Jira

У кожного таску є рівень сек'юрності (Security level). За допомогою цього рівня йде розмежування доступів до конкретних тасків вже всередині проекту. Тобто крім налаштованої схеми безпеки до проекту є також схема безпеки до тасків, тобто кожну задачу може бачити лише та людина, яка в ній приймає безпосередню участь або ж ті, хто мають повний доступ до проекту, так як це продемонстровано на рисунку (Рис. 3.5)..

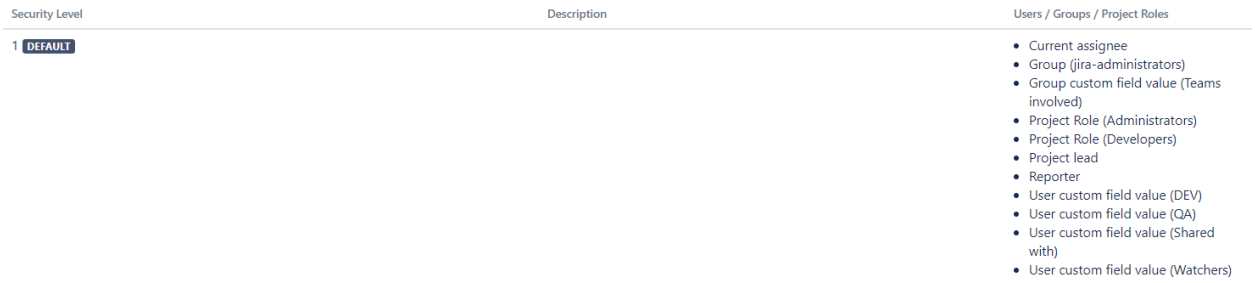

Рисунок 3.5. – Розмежування по рівню доступу до тасків

3.1.1. Confluence

Інформація зберігається не лише у JIRA, а й ще у Confluence. Confluence – локальна вікіпедія команда, де зберігається вся документація.

Confluence - це робоча область компанії, де знання та співпраця стикаються. Динамічні сторінки дають компанії місце для створення, захоплення та співпраці з будь-яким проектом чи ідеєю. Середовища допомагають структурі компанії, організовувати та ділитись роботою, тому кожен член команди має уявлення про знання в установі та доступ до інформації, необхідної для найкращої роботи. Конфлюенс стосується команд і компаній будь-якого розміру та типу, від тих, хто має критично важливі проекти з високими ставками, які потребують суворості за своїми практиками, до тих, хто шукає простір для побудови командної культури та взаємодії один з одним у більш відкритій та автентичний спосіб. Загальну структуру і приклад конфлюенса показано на скріншоті (Рис. 3.6.)

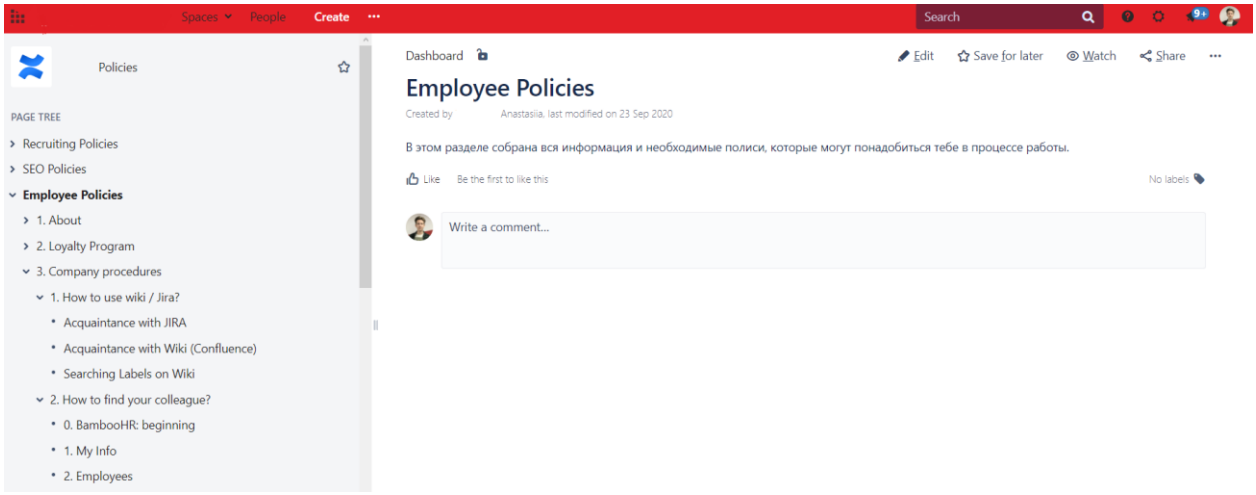

Рис. 3.6. – Приклад простору Confluence

Загальною структурою є поділ на простори(спейси), а в них поділ на сторінки. У кожного спейса/сторінки є також налаштовування доступів, що дозволяє

правильно розмежувати всіх членів компанії за правильною структурою у документаціях,(Рис. 3.7)..

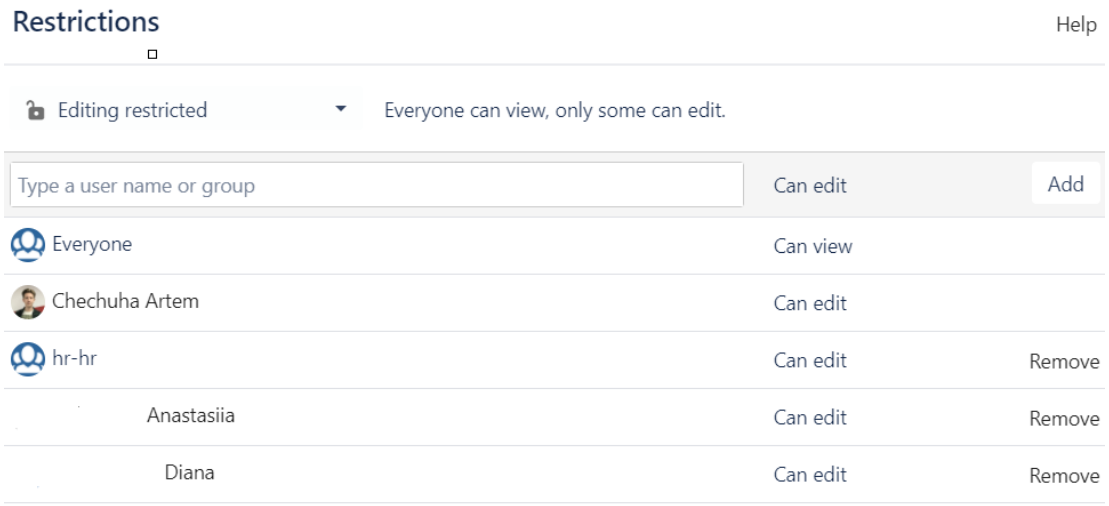

Рис. 3.7. – Розмежування доступів сторінки Confluence

3.1.2. LDAP

LDAP (Lightweight Directory Access Protocol) - це відкритий та кросплатформенний протокол, що використовується для аутентифікації служб каталогів.

LDAP дозволяє додаткам взаємодіяти з іншими серверами служб каталогів. Це важливо, тому що служби каталогів зберігають і передають важливу конфіденційну інформацію, пов'язану з користувачами, паролями і обліковими записами комп’ютерів.

Підключення Jira до LDAP Active Directory використовує структуру домену, щоб містити та впорядковувати інформацію про спільні ресурси, такі як сервери, томи, принтери та облікові записи: користувачів, груп та комп'ютерів. Він зберігає таку інформацію, як імена, паролі, номери телефонів тощо, і робить її доступною для пошуку. Тоді веб-програми можуть використовувати LDAP або полегшений протокол доступу до каталогів для пошуку цієї інформації. На ринку є кілька серверів LDAP, і, на щастя, Jira надає вбудовані роз’єми для найбільш популярних, таких як Microsoft Active Directory, Apache Directory Server, Fedora Directory Server і купа інших. У документації Atlassian є покроковий посібник із встановлення з'єднання LDAP. Незважаючи на те, що ми можемо інтегрувати

Jira з Active Directory, інтеграція за замовчуванням не вмикає синхронізацію атрибутів користувачів. Звичайно, ми можемо імпортувати їхні облікові записи вручну, але набагато простіше автоматично синхронізувати дані користувачів. Синхронізація атрибутів Active Directory - одна з програм, доступних на Atlassian Marketplace, яка дозволяє розширене використання даних LDAP у Jira. За допомогою встановленої програми ми можемо відображати атрибути користувачів у кількох місцях, а також виконувати деякі дії на сервері LDAP без необхідності пробудження адміністратора.

Весь облік юзерів та груп відбувається через LDAP, через групи юзери отримують доступ до JIRA та Confluence, та до відповідних проектів і середовищ у них. Системна структура компанії продемонстрована на рисунку (Рис. 3.8.)

Рисунок 3.8. - Системна структура компанії

3.2. Розробка системи управління ІБ

Так як найголовнішим інформаційним активом компанії є JIRA, було вирішено реалізувати систему видачі доступів до проектів/задач у JIRA, спейсів і сторінок у Confluence, тоюто загалом усієї інформації, що є в компанії на основі експертної оцінки, яка була проведена у розділі 2. Розробка програмного коду – скрипту була виконана за допомогою об’єктно-орієнтованної мови програмування Groovy. Groovy - об'єктно-орієнтована мова програмування, розроблена для платформи Java як доповнення до мови Java з можливостями Python, Ruby і

Smalltalk. Використовує Java-подібний синтаксис і безпосередньо працює з іншим Java-кодом і бібліотеками. Мова може використовуватися в будь-якому Java-проекті або як скриптова мова. Основними можливостями мови, що відрізняють його від Java: як статична, так і динамічна типізація; вбудований синтаксис для списків, асоціативних масивів, масивів і регулярних виразів; перевантаження операцій.

Виконується наступна логіка: при наймі нового співробітника у компанію, йому створюється обліковий запис у LDAP з загальними групами доступу, по цих групах він має певні базові мажливості, проте не має розширеного доступу до проектів. Якщо ж користувач потребує доступу до додаткового функціоналу, до повного перегляду задач в різних проектах, то він має звернутия до відповідального за це джира-адміністратора, а той у свою чергу має поставити задачу у проект EXS (Expert System), тип задачі – Access, у якому має заповнити наступні поля: Summary(коротка назва задачі), User who request access(вибір юзера хто запрошує доступ), Team(до якої команди належить юзер), Manager(чи юзер займає менеджерську позицію), Position(позиція у компанії), On probation(знаходиться юзер на випробувальному терміні або ні), Requested access group(група до якої потрібно видати доступ(Повний перелік груп і інформація про те, за якими групами куди доступ можна отримати знаходиться у Confluence і доступний лише адміністраторам)). Приклад створення задачі можна побачити на рисунках(Рис. 3.9), (Рис. 3.10)

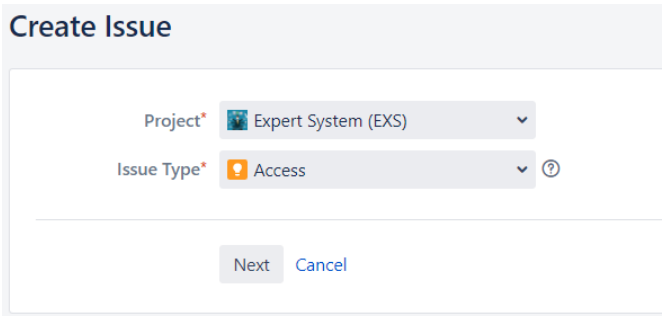

Рис. 3.9. – Створення таску на видачу доступу

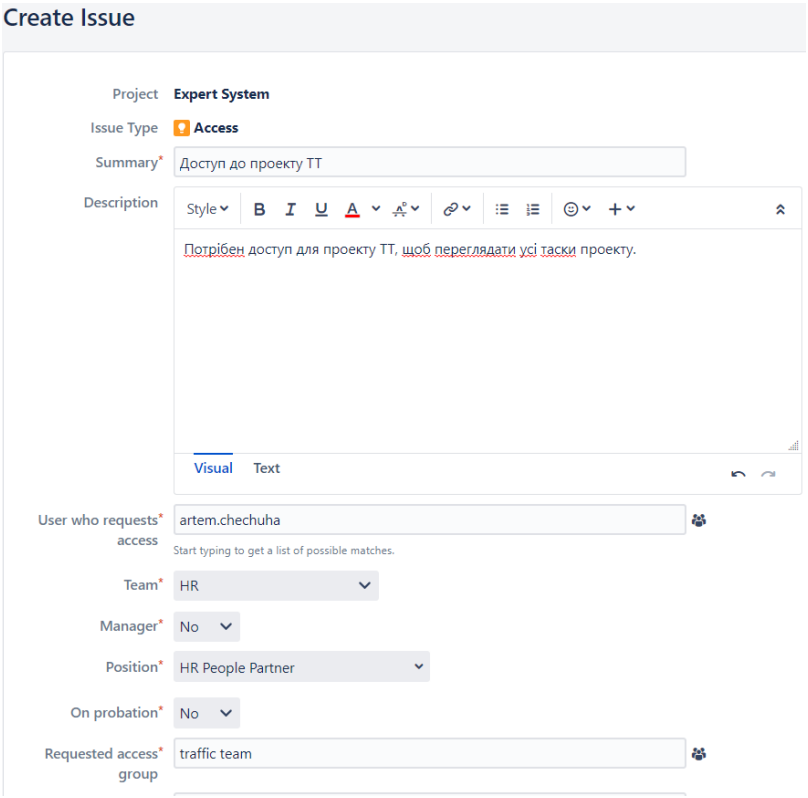

Рис. 3.10. – Розгорнуте створення таску на видачу доступів

Робочий процес, за яким виконується дана задача досить простий (Рис. 3.11.), тому що адміністратор має лише 2 варіанти рзвитку подій: видати доступ, або ж ні.

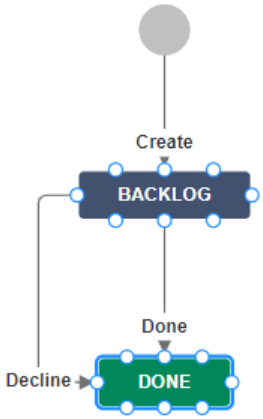

Рис. 3.11 – Робочий процес видачі доступів

Саме при створенні задачі і відпрацьовує наш скрипт “EXS Mark”,(Рис. 3.12.), який за допомогою перебору інформації, яку було введено при створенні задачі і видає результат.

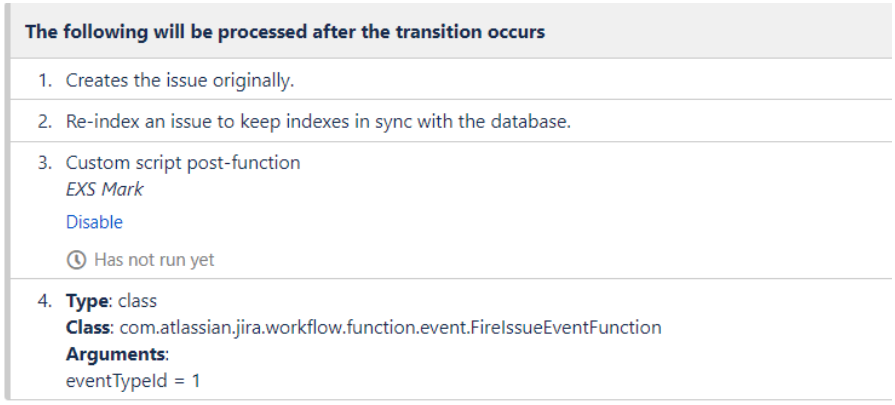

Рис. 3.12. – Вставлення скрипту програми при створенні задачі

Результатом нашого програмного коду є оцінка рівня загрози юзера для інформації (Expert Mark), (рисунок 3.13.), доступ до якої він зпрошує. Оцінка до 4х включно – загроза незначна, доступ можна отримати. Оцінка 5 і вище – загроза значна, доступ, на жаль, неможливий.

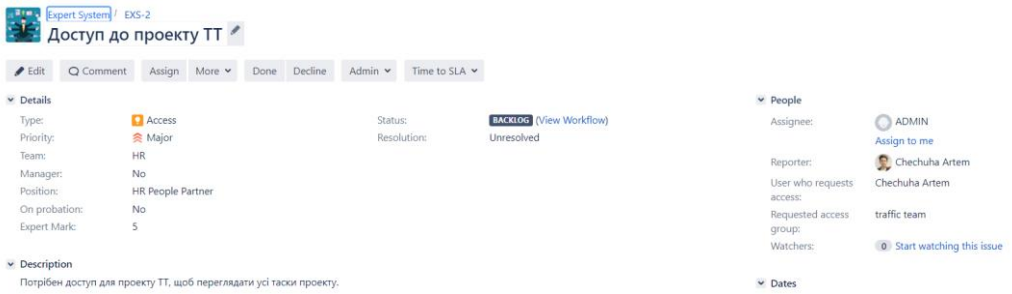

Рис. 3.13. – Результат програмного коду

На рисунках (Рис. 3.14.) і (Рис. 3.15.) також представлено приклади задач дял видачі доступів для юзерів з різними властивостями.

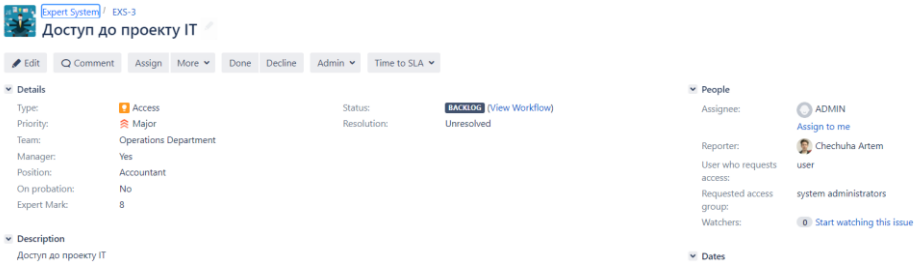

Рис. 3.14. – Результат програмного коду

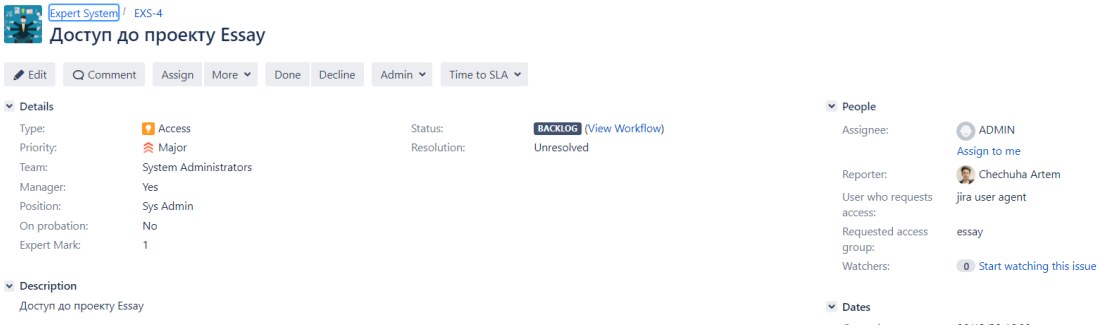

Рис. 3.15. – Результат програмного коду

Висновки до розділу 3

У розділі 3 даної дипломної роботи проведено огляд системного забезпечення, описано головні аспекти роботи JIRA/Confluence/LDAP. Продемонстрована схема зв’язку цих систем у підприємстві.

Розроблено програмний скрипт для системи управління інформаційною безпекою компанії за допомогою мови програмування Groovy. Наочно продемонстровано принцип роботи і управління даної системи.

ВИСНОВКИ

У ході досягнення мети дипломної роботи було виконано наступні завдання:

– Проведено огляд досліджень та нормативно-правової бази в галузі інформаційної безпеки та експертних систем;

– Побудована системи управління інформаційною безпекою на підприємтві середнього бізнесу;

– Проведена розробка програмного модулю для системи управління інформаційною безпекою на підприємтві середнього бізнесу.

Також досягли практичної цінності роботи, що полягає в покращені технології забезпечення захисту інформації на підприємстві середнього бізнесу шляхом впровадження експертної системи управління інформаційною безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хлапонін, Ю. І. Загальні характеристики загроз в кіберпросторі / Ю. І. Хлапонін, В. В. Овсяннiков, Н. А. Паламарчук // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: VI наук.-практ. сем. Військового інституту телекомунікацій та інформатизації НТУУ «КПІ», 20 жовтня 2011 р., 2011. — с. 157.

2. Хлапонін Ю.І. Управління інформаційною безпекою на основі інтелектуальних технологій / Ю.І. Хлапонін // Технологічний аулит та резерви виробництва. – П.: «Технологічний центр», 2014, — № 6/4(20).

3. Бойченко О. В. Модель корпоративного інформаційного захисту об'єкту інформатизації / О. В. Бойченко, Я. І. Торошанко // Наукові записки Українського науководослідного інституту зв'язку, 2011. – №4(20). – с. 15-19.

4. Бучик С.С. Методика оценивания информационных рисков в автоматизированной системе / С.С. Бучик, С.В. Мельник //Збірник наукових праць ЖВІ ДУТ. – 2015. - № 11. – с.33-43

5. Журан О.А. Необхідність управління інформаційною безпекою на підприємстві [Електронний ресурс] / О.А. Журан, О.В.Бучка. - О.: Одеський національний політехнічний університет, 2017. - Режим доступу: http://dspace.opu.ua/jspui/bitstream/123456789/7135/1/необхідність%20управління%20інформаційною%20безпекою%20на%20підприємстві.pdf.

6. Довбня С.Я. / Особливості та методика створення експертної системи підтримки прийняття рішень щодо управління комплексною безпекою інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності / С.Я. Довбня, Ю.А. Хлапонін, С.В. Биков, І.Ю. Четверіков // Сучасний захист інформації. – 2013. - №1. – с.24

7. Бурдин О. А. Комплексная экспертная система управления информационной безопасностью «АванГард» / О. А. Бурдин, А. А. Кононов // Информационное общество, 2002. – №3. – Вып. 1. – с. 9

8. Жигулін Г.П. Методичний підхід до прогнозування інформаційних атак, як загроз автоматизованим системам управління / Г.П.Жигулін, Ю.А.Печеневський // Проблеми інформаційної безпеки. Комп'ютерні науки, 2000. - № 2. - С. 60-63.

9. Будько М.Б. Відслідковування змін в структурі мережі і рішення задач забезпечення ІБ на основі аналізу потоків даних / М.Б. Будько, М.Ю Будько // Науково-технічний вісник інформаційних технологій, механіки та оптики, 2009. - № 1(59). - С. 78-82.

10. Симонов С.В. Анализ рисков, управление рисками / С.В. Симонов // JetInfo. - 1999. - № 1. – С. 28

11. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты / С.В.Симонов // Защита информации. - 2001. - №2. – С. 53

12. Анісімов О.О. Менеджмент в сфері информаційної безпеки / О.О. Анісімов -М.: Інтернет – університет інформаційних технологій, 2010 – 176 с.

13. Уілсон Е. Моніторинг і аналіз мереж. Методи виявлення несправностей / Е. Уілсон. - М.: «ЛОГІ». 2012 – 176 с.

14. Уотермен Д. Керівництво по експертним системам / Д. Уотермен; пер. з англ. В.Л. Стефанюка. – М.: «Мир». - 1989. - 388с.

15. Джарратано Дж. Экспертные системы. Принципы разработки и программирование / Дж. Джарратано, Г. Райли. - М.: Издат. дом «Вильямс», 2007. – 1152 с.

16. Суменков М.С. Экспертные системы при принятии решений на предприятии [Електронний ресурс] / М.С. Суменков //Бизнес.Менеджмент.Право, 2003. - №2. - Режим доступу: http:// bmpravo.ru/show_stat.php?stat=193

17. Бази знань інтеллектуальних систем: підручник / за ред. Т.О.Гаврілова, В.Ф. Хорошевський. - СПб.: Пітер, 2000. - 384 с

18. Фохт Д. Проектування та програмна реалізація експертних систем на персональних ЕВМ / Д. Фохт, К. Таунсенд; пер. з англ. В. О. Кондратенко, С. В. Трубіцина — М.: Фінанси та статистика, 1990. - 320 с.

19. Трахтенгерц Е.О. Комп'ютерні системи підтримки прийняття управлінських рішень / Е.О. Трахтенгерц // Проблеми управління. – К.: Інститут космічних досліджень НАН та НКА України, 2013, - №1, - с. 13 -27.

20. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів [Електроний ресурс]: ДП УкрНДНЦ наказ від 16.10.2019 р. № 312. – Режим доступу: http://online.budstandart.com/ua/catalog/docpage.html?id_doc=85795

21. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги [Електроний ресурс]: ДП УкрНДНЦ наказ від 18.12.2015 р. № 193. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910

22. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки [Електроний ресурс]: ДП УкрНДНЦ наказ від 18.12.2015 р. № 193. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911

23. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова [Електроний ресурс]: ДП УкрНДНЦ наказ від 24.09.2018 р № 337. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=78517

24. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання [Електроний ресурс]: ДП УкрНДНЦ наказ від 24.09.2018 р. № 337. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=78518

25. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Електроний ресурс]: ДП УкрНДНЦ наказ від 18.12.2015 р. № 193. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

26. ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою» [Електроний ресурс]: ДП УкрНДНЦ наказ від 18.12.2015 р. № 193 – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66913

27. ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Мастанова щодо аудиту систем керування інформаційною безпекою [Електроний ресурс]: ДП УкрНДНЦ наказ від 10.12.2018 р. № 470. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80303

28. ДСТУ ISO/IEC 27011:2018 Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002 [Електроний ресурс]: ДП УкрНДНЦ наказ від 24.09.2018 р. № 337. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=78519

29. Офіційний сайт ISO [Електронний ресурс]. – Режим доступу: https://www.iso.org/ru/news/ref2450.html

30. Офіційний сайт ISACA. COBIT [Електроний ресурс]. – Режим доступу https://www.isaca.org/resources/cobit/

31. Information technology. Security techniques. Information security management. Measurement: ISO/IEC 27004:2016 [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/64120.html

32. Information technology. Security techniques. Information security management. Measurement: ISO/IEC 27004:2016 [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/64120.html

33. Information technology. Security techniques. Information security management. Measurement: ISO/IEC 27004:2016 [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/64120.html

34. Заде Л. Поняття лінгвістичної змінної і її застосування до прийняття наближених рішень / Л.Заде. − М.: Мир, 1976. − 166 с.