Київський національний торговельно-економічний університет

Кафедра комп’ютерних наук

ВИПУСКНИЙ КВАЛІФІКАЦІЙНИЙ ПРОЕКТ
на тему:

«Програмна реалізація моделі захисту даних Digital Agency «Q-SEO»»

Студентки 4 курсу, 11 групи,
факультету обліку, аудиту та
інформаційних систем, денної
форми навчання
напрям підготовки
«Комп’ютерні науки» _____ Москалюк Івanни Юріївни

Науковий керівник
кандидат фіз.-матем. н.
доцент _____ Самойленко Анна Тимофіївна

Гарант освітньої програми
кандидат техн. наук
доцент _____ Демідов Павло Георгійович

Київ 2019

ЗМІСТ

АНОТАЦІЯ

Москалюк І.Ю. Програмна реалізація моделі захисту даних Digital Agency «Q-SEO»

Дослідження присвячене реалізації моделі захисту даних Digital Agency «Q-SEO» від несанкціонованого доступу в програмному середовищі BizAgi Modeler.

У випускному кваліфікаційному проекті описано оптимальний процес організації захисту даних на підприємстві за сукупністю і взаємозв'язку всіх видів і напрямків захисту даних. Створено та реалізовано модель захисту даних від несанкціонованого доступу.

ABSTRACT

Moskaliuk I. Software implementation of the Digital Agency Data Protection Model "Q-SEO"

The research is devoted to the implementation of the Digital Agency Data Protection Model "Q-SEO" from unauthorized access in the BizAgi Modeler software environment.

The graduation qualification project describes the optimal process of data protection organization at the enterprise in the totality and interconnection of all types and areas of data protection. A model for protecting data from unauthorized access was created and implemented.

ВСТУП

Ефективний захист даних - це одна з важливих сучасних проблем. З поширенням інформаційних технологій організації стають усе більш залежними від інформаційних систем та послуг. Тому проблема захисту даних в наші дні стоїть особливо гостро. Забезпечення необхідного рівня захисту даних задача досить складна, що вимагає для свого рішення створення цілісної системи організаційних заходів і застосування специфічних засобів та методів із захисту даних.

Використання різних методик з метою оцінювання захисту інформації на підприємствах розглядали багато вчених, а саме: В. В. Бут, В. В. Микитенко, О. В. Гребенюк, М. О. Живко, О. А. Сороківська, В. С. Цимбалюк, А. М. Чорна. Проте нерозв’язаним питанням у сфері захисту інформації залишається обґрунтування необхідності використання моделей та методів дослідження. Сучасні методи не завжди є доступними та зручними у використанні, потребують значних матеріальних витрат

Одним з основних елементів захисту є саме моделі захисту даних. Вони є складовими частинами загального процесу моделювання, який можна поділити на дві складові: побудова та реалізація моделі.

Основною метою роботи є розробка та програмна реалізація моделі захисту даних на підприємстві.

Об'єктом дослідження є захист даних Digital Agency «Q-SEO».

Предмет дослідження - модель захисту даних від несанкціонованого доступу.

Мета роботи полягає в огляді та аналізі існуючих моделей захисту даних, створенні загальної моделі захисту даних на підприємстві та реалізації моделі СЗІ від НСД за допомогою програмних засобів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ДАНИХ

1. Захист даних

Будь-яка діяльність людини базується на даних. У контексті автоматизованої обробки даних та інформаційних систем термін "дані" має надзвичайно важливе значення і від правильної його інтерпретації залежить ефективність людино-машинних систем.

Інформація — це відомості про навколишній світ (об'єкти, явища, події, процеси тощо), які зменшують міру наявної невизначеності, неповноти знань, відчужені від їх творця та які стали повідомленнями (вираженими певною мовою у вигляді знаків, у тому числі й записаними на матеріальному носії). [20]

Обов'язкові атрибути інформації: наявність носія, джерела і приймача, а також каналів зв'язку між ними (Рис. 1.1).

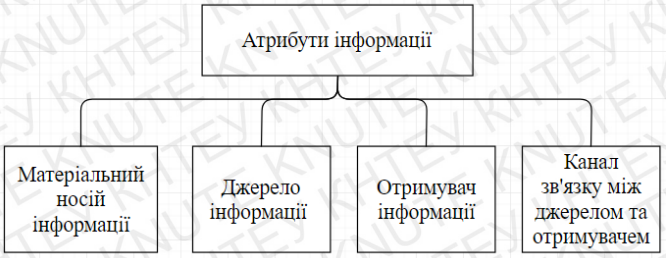

Рис. 1.1. Атрибути інфомації

Дані — це дані, подана у формалізованому вигляді, прийнятому для опрацювання автоматичними засобами за можливої участі людини (вхідні, вихідні дані, база даних тощо).[16]

Виходячи з наведених визначень, співвідношення понять "інформація" і "дані" можна відобразити такою схемою (Рис. 1.2):

Рис. 1.2. Співвідношення інформації та даних

За́хист даних (англ. *Data protection*) — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації/даних за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам даних (даних).[15]

Процес захисту даних - це процес взаємодії загроз, що впливають на інформацію, і засобів захисту даних, які перешкоджають їх впливу .

У загальному вигляді модель процесу захисту даних в ІС може бути представлена так, як це показано на Рис. 1.3.

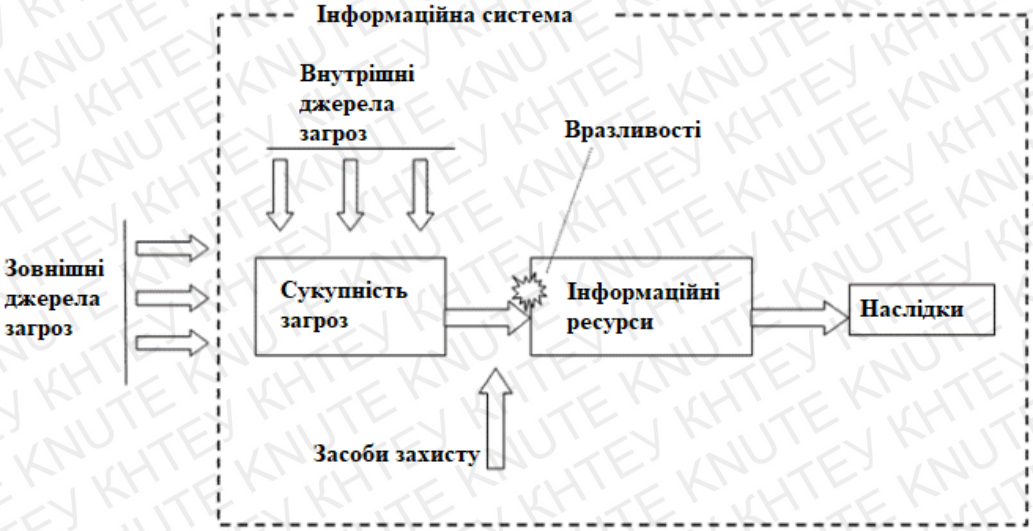

Рис.1.3 -Загальна модель процесу захисту даних

Процес захисту даних необхідно також розглядати як процес розподілу ресурсів, виділяються на захист даних. Оптимальний вибір засобів захисту представляється непростим завданням, яку у подальший планується вирішити, створивши вдосконалену модель використання та розподілу ресурсів, що виділяються на захист даних.[21]

2. Моделі захисту даних

Основне призначення моделей – це створення умов для об'єктивної оцінки загального стану інформаційної системи з точки зору міри уразливості або рівня захищеності даних в неї.[19]

Як і будь-яка інша сфера, інформаційна безпека також з самого початку свого виникнення почала розглядатися на предмет можливості застосування в ній методів моделювання. Історично першими виникли і досить детально вивчалися моделі безпеки.

В основному розглядаються моделі, появу яких можна вважати суттєвими кроками або етапами в теорії та практиці захисту даних. Тобто моделі, в яких запропоновано принципово нові ідеї. [9]

2.1. Модель ADEPT-50

Одною з перших спроб використати математичну модель для опису механізму захисту була модель ADEPT-50, яка була вперше опублікована в 1970 році. Вона включає чотири типи об’єктів, що мають відношення до безпеки: користувачі, завдання, термінали і файли, причому кожний з об’єктів описується певною чотирьохмірною структурою (автори називали її кортежем) (A,C,F,M), який містить основні параметри безпеки.

2.2. Модель HRU

Розробку моделі HRU (Harrison M., Ruzzo W., Ullman J.), теж слід вважати важливим етапом в розвитку теорії захисту даних. Модель HRU використовується для аналізу системи захисту, яка реалізує дискреційну політику безпеки і її основного елемента – матриці доступів. Система захисту представляється кінцевим автоматом, що функціонує відповідно до певних правил переходу. Модель HRU була вперше запропонована в 1971 році.

2.3. Модель Take-Grant

Модель розповсюдження прав доступу Take-Grant, що була запропонована в 1976 році, використовується для аналізу систем дискреційного розмежування,

доступу в першу, чергу для аналізу шляхів розповсюдження прав доступу в таких системах. В якості основних елементів моделі використовуються графи доступів і правила їх перетворень. Мета моделі – дати відповідь на питання про можливість отримання прав доступу суб'єктом системи на об'єкт в стані, що описується графом доступів. В подальшому модель Take-Grant отримала продовження як розширена модель Take-Grant, в якій розглядаються шляхи виникнення інформаційних потоків в системах з дискреційним розмежуванням доступу.[14]

2.3.1. Модель Белла-ЛаПадула

Основним положенням даної моделі, є призначення усім учасникам процесу обробки даних, що захищається, і документам, в яких вона міститься, спеціальної мітки, наприклад, таємно, цілком таємно і т. д., що отримала назву рівня безпеки. Всі рівні безпеки впорядковуються за допомогою встановленого відношення домінування. Контроль доступу здійснюється залежно від рівнів безпеки взаємодіючих сторін на основі двох простих правил: [7]

1. Уповноважена особа (суб'єкт) має право читати тільки ті документи, рівень безпеки яких не перевищує його особистий рівень безпеки.
2. Уповноважена особа (суб'єкт) має право заносити інформацію тільки в ті документи, рівень безпеки яких не нижче його особистого рівня безпеки.

2.3.2. Моделі цілісності

Інша важлива властивість захищеної даних – цілісність також стала предметом моделювання. Тут розглянемо дві моделі цілісності – модель Кларка-Вілсона і модель Біба.

Модель цілісності Кларка-Вілсона була запропонована в 1987 р. як результат аналізу практики паперового документообігу, ефективної з точки зору забезпечення цілісності даних. Модель Кларка-Вілсона є описовою і не містить строгих математичних конструкцій.

Модель Біба була розроблена в 1977 році як модифікація моделі Белла-ЛаПадули, орієнтована на забезпечення цілісності даних. [12]

Базові правила Моделі Біба формулюються таким чином:

1. Просте правило цілісності (Simple Integrity, SI). Суб'єкт з рівнем цілісності x_S може читати інформацію з об'єкта з рівнем цілісності x_O тоді і тільки тоді, коли x_O має перевагу над x_S.
2. * - властивість (* - integrity). Суб'єкт з рівнем цілісності x_S може писати інформацію в об'єкт з рівнем цілісності x_O тоді і тільки тоді, коли x_S має перевагу над x_O.

2.3.3. Моделі загального типу

В моделях загального типу основним є не тільки питання доступу суб'єктів до об'єктів, а інші аспекти безпеки. До них належаль:

- Модель процесу захисту
- Модель системи захисту
- Модель функцій захисту
- Модель з повним перекриттям
- Інформаційно-аналітична модель з оцінки захисту даних від загроз НСД

Висновки до розділу 1:

Застосування моделей, як спрощених описів важливих компонентів системи, дає змогу спростити розв'язок завдання створення адекватної реальним загрозам системи захисту.

Розглянуті вище моделі використовують для опису механізму захисту, для аналізу системи захисту, для аналізу систем дискреційного розмежування, для контролю доступу, для забезпечення цілісності даних, тощо.

РОЗДІЛ 2. ОСНОВИ ЗАХИСТУ ДАНИХ НА ПІДПРИЄМСТВІ

2.1. Організація захисту даних на підприємстві

Організація захисту даних на підприємстві (ОрЗІ) є найважливішою складовою розробки системи захисту даних на підприємстві. Однак, існуючі моделі ОрЗІ в недостатній мірі чітко і ясно формують уявлення про її структуру, склад і зміст, що створює серйозну проблематику забезпечення інформаційної безпеки організації. У зв'язку з цим, з метою підвищення ефективності забезпечення інформаційної безпеки організації очевидна постановка завдання про розробку моделі організації захисту даних на підприємстві. [17]

Захист даних є прийняття правових, організаційних і технічних заходів, спрямованих на:

1. забезпечення захисту даних від незаконного втручання, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій у відношенні такої даних;
2. отримання конфіденційності даних обмеженого доступу;
3. реалізацію права на доступ до даних.[16]

Види ЗІ визначаються наступним чином:

- *правовий захист даних*: Захист даних правовими методами, що включає в себе розробку законодавчих і нормативних правових документів (актів), що регулюють відносини суб'єктів щодо захисту даних, застосування цих документів (актів), а також нагляд і контроль за їх виконанням;
- *технічний захист даних*; ТЗІ: Захист даних, яка полягає в забезпеченні некриптографічними методами безпеки даних (даних), що підлягає (підлягають) захисту відповідно до чинного законодавства, із застосуванням

технічних, програмних і програмно-технічних засобів;

- *криптографічний захист даних*: Захист даних за допомогою її криптографічного перетворення;
- *фізичний захист даних*: Захист даних шляхом застосування організаційних заходів та сукупності засобів, що створюють перешкоди для проникнення або доступу неуповноважених фізичних осіб до об'єкта захисту.

З системних позицій концепт моделі взаємозв'язку видів захисту даних може бути представлений таким чином:

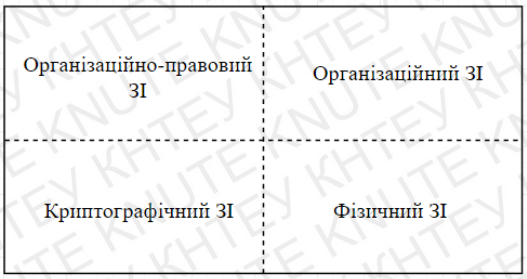

Рис. 2.1. Концепт моделі взаємозв'язку видів захисту даних

Напрямки ЗІ сформовані в відомій моделі захисту даних [3], концепт якої представлений на Рис.2.2.

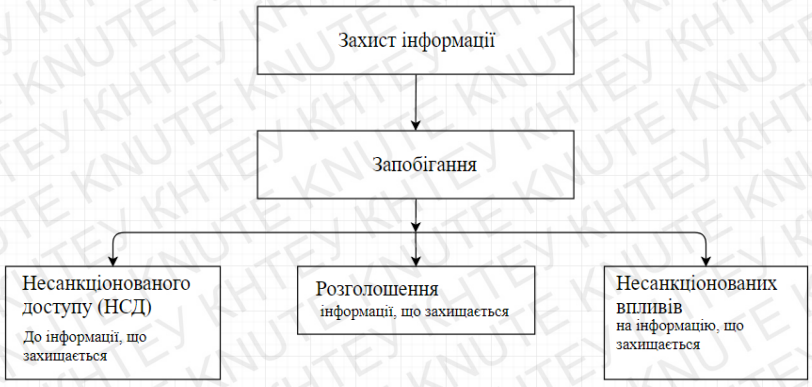

Рис. 2.2. Концепт оптимальної моделі захисту даних

Представлена модель захисту даних в загальному зрозуміла, проте вимагає додаткових уточнень, якими основними способами можуть здійснюватися несанкціонований доступу до даних, розголошення та несанкціонований вплив на інформацію, що захищається.[18]

Захист даних від несанкціонованого доступу; ЗІ від НСД: Захист даних, спрямований на запобігання отримання даних, що захищається, зацікавленими суб'єктами з порушенням встановлених нормативними та правовими документами (актами) або власниками даних прав або правил розмежування доступу до даних, що захищається.

Захист даних від розголошення: Захист даних, спрямована на запобігання несанкціонованого доведення даних, що захищається до зацікавлених суб'єктів (споживачів), які не мають права доступу до цієї даних.

Захист даних від несанкціонованого впливу; ЗІ від НСВ: Діяльність, спрямована на запобігання впливу на інформацію, що захищається, з порушенням встановлених прав і (або) правил зміни даних, що приводить до знищення, перекручення, збою в роботі, блокування доступу до даних, а також до втрати, знищення або збою функціонування носія даних. [11]

Аналіз змісту несанкціонованого доступу до даних дозволяє виділити наступні основні способи його здійснення:

- перехоплення даних технічними каналами витоку даних;
- несанкціонований доступ до даних в АС/ІС (автоматизованих/інформаційних системах);
- втрата (викрадення/втрату) носія даних, розуміючи під викраденням крадіжку, грабіж або розбій;
- отримання даних розвідками.

ЗІ від НСВ включає такі способи захисту даних як захист даних від навмисного впливу і захист даних від ненавмисного впливу. Причому, ненавмисний вплив на інформацію, що захищається, включає в себе помилки користувача, збої програмних і технічних засобів, вплив природних явищ та інших, не цілеспрямованих на зміну даних, подій. [13]

Таким чином, модель захисту інформації може бути представлена в наступному вигляді (Рис.2.3)

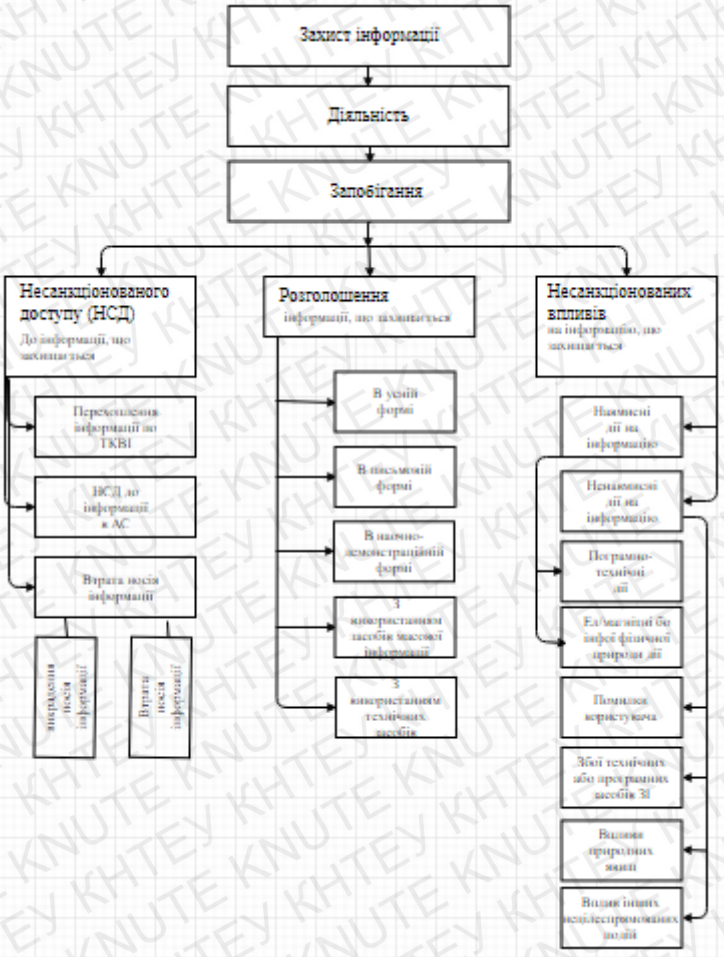

Рис. 2.3. Модель захисту інформації

Викладене дозволяє представити концепт моделі ОрЗІ наступним чином:

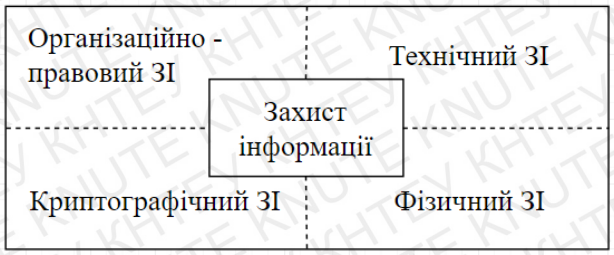

Рис. 2.4. Концепт моделі взаємозв'язку видів захисту інформації

А також визначити, що організація захисту даних здійснюється за сукупністю і взаємозв'язку всіх видів і напрямків захисту даних.

2.2. Опис програмного забезпечення для розробки моделі захисту даних

Робота будь-якого інженера, IT-фахівця, маркетолога, бізнес-аналітика,

менеджера пов'язано з необхідністю створення різних діаграм, блок-схем і графіків. Моделі у даному випускному кваліфікаційному проекті створені у наступних сервісах:

- Draw.io;
- BizAgi Modeler.

Draw.io - це сервіс, призначений для формування діаграм і схем. Сервіс розділений на три частини - меню, панель об'єктів і сам документ.

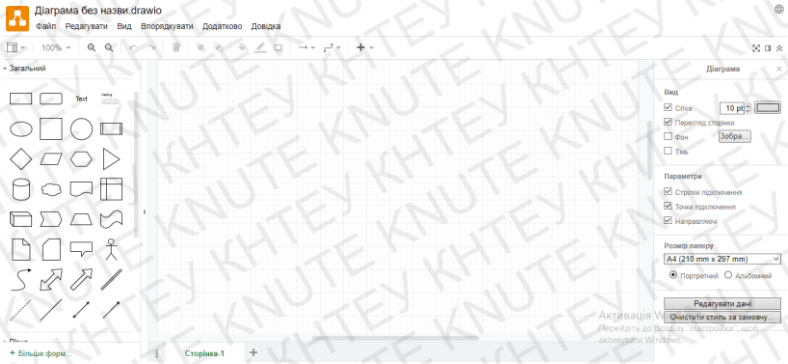

Рис. 2.4. Робоча поверхня сервісу Drow.io

За допомогою редактора можна створювати будь-які схематичні зображення - від схем електричних ланцюгів до структур бізнес-моделей. У числі можливостей - побудова діаграм, графіків і UML-моделей. У бібліотеці форм присутні кілька десятків фігур, згрупованих за категоріями. Об'єкти можна форматувати, змінюючи шрифти, колір, градієнт, товщину ліній, рівень прозорості. Завдяки можливості синхронізації з Google Диском над документами можуть одночасно працювати кілька користувачів. Готові зображення можна зберігати на жорсткому диску ПК або вставляти в вікі-сайти і блоги. Доступні формати для експорту - PDF, GPG, SVG, XML і JPG.

Ключові особливості:

- Безкоштовна інтеграція з сервісами Google;
- Платна інтеграція з Confluence і JIRA Cloud;
- HTML клієнт з підтримкою IE 6-8;
- Підтримка смартфонами і планшетами;

- Експорт документів у формати PDF, GPG, SVG, XML і JPG;
- Оффлайн додаток для Windows, MacOS і Linux;
- Підтримка 27 мов.

Його головна перевага - безкоштовність. Крім того, для повноцінної роботи не потрібно проходити реєстрацію і проходити процес авторизації на сайті.[3]

Bizagi Suite - це BPM-система, розроблена однойменною компанією, і спрямована на моделювання, виконання, автоматизацію і аналіз бізнес-процесів. Система Bizagi включає 3 модуля для повноцінної настройки процесів:

- Modeler - повнофункціональна середу моделювання процесів в нотації BPMN;
- Studio - середовище розробки бізнес-процесів;
- Engine - середовище виконання процесів, яка доступна користувачам в будь-якому браузері з будь-якого пристрою.

Bizagi Modeler - це частина вищезгаданого BizAgi Suite. Програма незалежна від повного комплекту і може бути поставлена окремо.

Дуже простий, лаконічний і зручний інтерфейс (Рис. 2.5).

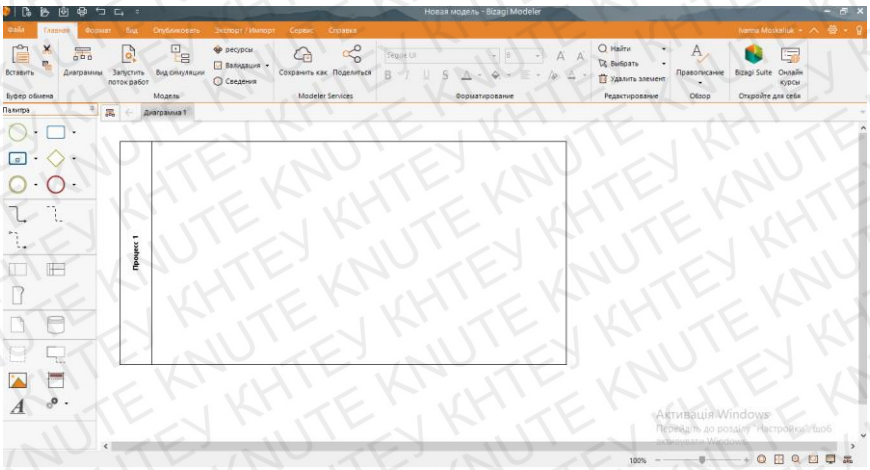

Рис. 2.5. Інтерфейс BizAgi Modeler

Моделі, побудовані в BizAgi Modeler, повністю сумісні з повною версією - Suite. Створений в Modeler бізнес-процес можна редагувати, зберегти, експортувати в різних форматах (pdf, html).

Моделювання бізнес-процесу проводиться в форматі BPMN 2.0. Цей формат дещо відрізняється від відомого багатьом BPMN 2.0, зате в Bizagi є власні розробки, яких не має в інших системах, наприклад, Mailstone - проміжний етап.[8]

Створені в Modeler карти бізнес-процесів можна як "поширювати" на порталі Bizagi, так і використовувати коллаборатів, тобто кілька співробітників можуть виконувати спільну роботу, що дуже зручно.

Modeler має російськомовний варіант інтерфейсу, на відміну від двох інших модулів.

Bizagi Modeler призначений тільки для моделювання бізнес-процесів. Тобто якщо необхідний тільки дизайн бізнес-процесу, цього модуля буде досить. Якщо ж необхідно не тільки моделювати, але і розробляти та виконувати бізнес-процеси, то знадобиться модуль Studio, в якому є свій моделер бізнес-процесів.

Функціонал і особливості:

- нотація BPMN;
- перевірка моделей;
- автоматична генерація документів;
- управління атрибутами елементів моделей;
- можливість додавати свої елементи в моделі;
- вивантаження моделі в графічному вигляді;

Висновки до розділу 2.

У даному розділі було проаналізовано зміст поняття захист даних, види захисту даних, на основі чого створено концептуальну модель ЗІ.

Обраними програмними засобами для створення моделей - Drow.io та BizAgi Modeler - можна створювати будь-які схематичні зображення - від схем електричних ланцюгів до структур бізнес-моделей. Вони легкі в освоюванні, кожна містить свій функціонал та власні розробки, чим відрізняються від освеєних систем під час навчання.

РОЗДІЛ 3. РОЗРОБКА ТА РЕАЛІЗАЦІЯ МОДЕЛІ ЗАХИСТУ ДАНИХ

3.1. Розробка системи захисту даних на підприємстві.

У загальному випадку система захисту даних визначається як сукупність органів і (або) виконавців, техніки захисту даних, що використовується ними, а також об'єктів захисту даних, організована і функціонує за правилами і нормами, встановленими відповідними документами в галузі захисту даних. [1]

Це дозволяє представити концепт моделі СЗІ (Рис. 3.1).

Запропонована модель є узагальненою, тому вимагає уточнення і актуалізації в задачах розробки СЗІ на підприємстві.

Рис. 3.1. Концепт моделі системи захисту даних

В основі складової «Органи» визначаються органи з атестації об'єктів інформатизації (ОІ) і аудиторських фірм, головною організацією підприємства.

В якості складової «Виконавці» вважається обгрунтованим визначити керівника підприємства і службу інформаційної безпеки організації.

Складовою «Техніка захисту даних» визначено як засоби захисту

даних, в тому числі кошти фізичного захисту даних, криптографічні засоби захисту даних, засоби контролю ефективності захисту даних, засоби і системи управління, призначені для забезпечення захисту даних.

Як «Об'єкти захисту даних» відповідно до раніше запропонованої моделі об'єкта захисту даних визначено об'єкти інформатизації підприємства (ОІ).

Більш детальний аналіз СЗІ дозволяє зробити обґрунтований висновок про те, що сукупність складових «Організована» і «Функціонуюча» становлять систему менеджменту інформаційної безпеки (СМІБ) підприємства (Рис. 3.2). За основу СМІБ прийнято циклічну модель Демінга [7], яка представлена сукупністю чотирьох груп взаємопов'язаних процесів. [2]

Модель СМІБ представляється досить зрозумілою, проте при розробці СЗІ на підприємстві вимагає уточнення змісту груп процесів «Реалізація» і «Перевірка» (Рис. 3.2).

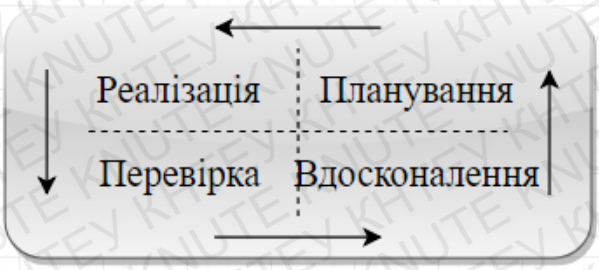

Рис. 3.2. Модель системи менеджменту ІБ.

За основу групи процесів «Реалізація» прийняті модель захисту даних [6] і поняття організації захисту даних, яка здійснюється за сукупністю і взаємозв'язку всіх видів і напрямків захисту даних. Такий підхід представлений на Рис. 3.3.

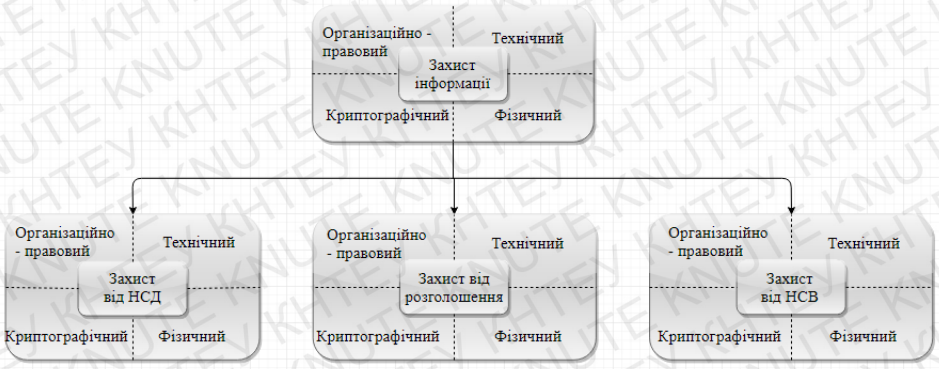

Рис. 3.3. Модель реалізації захисту даних

Основу групи процесів «Перевірка» становить комплекс організаційно-технічних заходів, що включає відомчий, позавідомчий контроль і аудит на основі сукупності експертно-документального, розрахунково-інструментального контролю, а також шляхом санкціонованого злому СЗІ (в тому числі пентестінга). При цьому передбачається проведення контролю в плановому і позаплановому порядку. Очевидно, що проведення контролю здійснюють структури, зазначені вище в підрозділі «Органи» (не виключаючи перевірки з боку органів вищого рівня). Це дозволяє представити модель групи процесів «Перевірка» (Рис. 3.4).

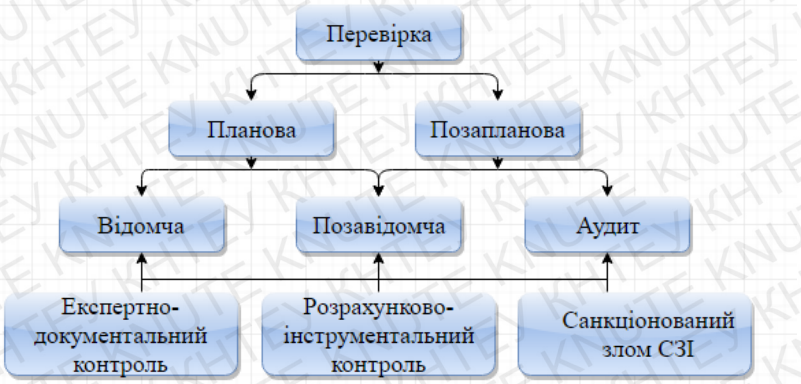

Рис. 3.4. Модель групи процесів «Перевірка»

На основі викладеного модель СЗІ на підприємстві можна представити на рис. 3.5.

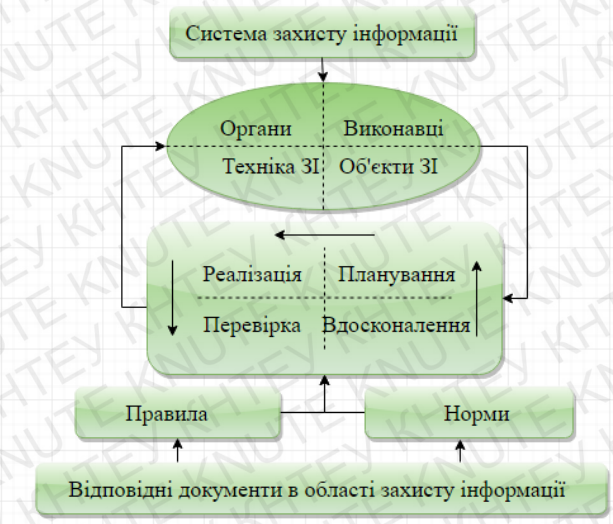

Рис. 3.5. Модель СЗІ на підприємстві

3.2. Розробка моделі захисту даних від НСД

У випускному кваліфікаційному проекті розроблено модель СЗІ від несанкціонованого доступу (НСД), концептуальна модель якої (рис. 3.6) створена за допомогою сервісу Drow.io.

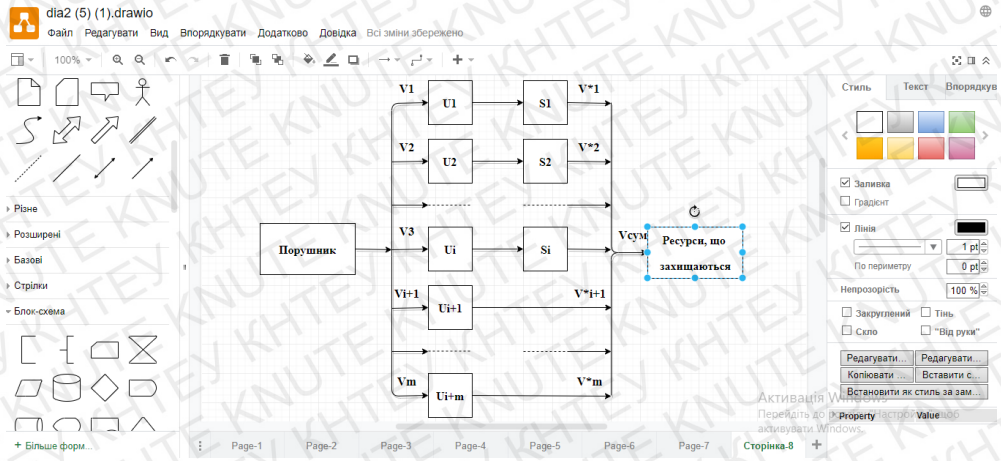

Рис. 3.6. Модель СЗІ від НСД

СЗІ представлена у вигляді мережевої моделі, що складається з певного набору засобів захисту S_i. На вхід засобів захисту надходять потоки запитів НСД, що визначаються моделлю порушника на безлічі потенційних загроз $\{U_i\}$. Кожен з засобів захисту відповідає за захист від загрози певного типу і використовує

відповідний захисний механізм. Його завдання полягає в тому, щоб розпізнати загрозу і заблокувати несанкціонований запит. [10]

В результаті функціонування системи захисту початковий потік НСД розріджується, утворюючи вихідний потік. Вхідні потоки несанкціонованих запитів позначені як $V_i(t)$, i=1,...,n, а потоки нерозпізнаних (пропущених) системою захисту НСД - V_i'. Факт неповного закриття системою захисту всіх можливих каналів прояви загроз враховується відсутністю для m вхідних потоків засобів захисту, що означає $V_i'(t)=V_i(t)$. Потоки запитів на НСД, що надходять по і-их каналах, розріджуються з вірогідністю $p_i(y)$, які залежать від використовуваного способу виявлення та блокування несанкціонованого доступу.

На виході СЗІ утворюється вихідний потік, який є об'єднанням вихідних потоків і-засобів захисту і потоку НСД-запитів, що приходять по m неконтрольованих каналах.

Кожне засіб (механізм) захисту характеризується ймовірністю пропуску НСД - q i, відповідно, ймовірністю забезпечення захисту (відображення НСД):

$$p = 1-q. \quad (3.1)$$

Порушник характеризується вектором інтенсивностей

$$\lambda = \{\lambda_1, \lambda_2, \dots \lambda_{i+m}\} \quad (3.2)$$

спроб реалізації відповідних загроз $U_1 \dots U_{i+m}$.

Для реалізації системного підходу до вирішення проблеми забезпечення інформаційної безпеки необхідно комплексне використання методів моделювання систем і процесів захисту даних. Цілями такого моделювання є пошук оптимальних рішень управління механізмами захисту, оцінки ефективності використання засобів і методів захисту і т.п.

Модель представляє логічний або математичний опис компонентів і функцій, що відображають істотні властивості модельованого об'єкта або процесу.

Для побудови моделі СЗІ за допомогою системи BizAgi Modeler необхідно співвіднести структурні елементи вихідної моделі з функціональними

блоками моделюючої системи, що їх замінюють.

З метою ідентифікації функціональних блоків моделі представимо математичну модель СЗІ, показану на Рис. 3.6 , у вигляді концептуальної моделі, що складається з трьох основних блоків: «Порушник», «СЗІ» і «ресурси, що захищаються» (Рис. 3.7).

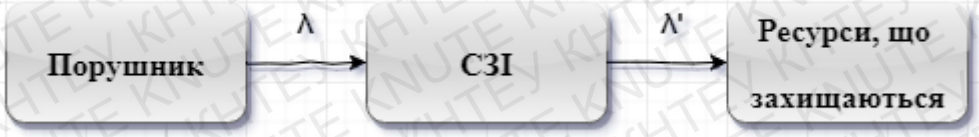

Рис. 3.7. Спрощена концептуальна модель СЗІ від НСД

«Порушник» є першим блоком моделі і в загальному випадку не піддається вхідному впливу. Завдання функціонування цього блоку - генерація потоку (потоків) запитів НСД (транзактів) із заданою інтенсивністю λ. Відповідно до моделі порушника, зловмисник намагається реалізовувати різні загрози захищеності даних з відповідними інтенсивностями.

Блок «СЗІ» показує функціонування СЗІ від НСД (МЗ). Елементи цього блоку можуть імітувати черги запитів НСД на входах механізмів захисту (МЗ), затримки на обслуговування, вихід МЗ з ладу (апаратної частини) і т.д. Однак головним завданням функціонування цього блоку є відсіювання запитів НСД з певною (заданою) ймовірністю. Розріджений потік запитів НСД на виході блоку «СЗІ» має інтенсивність λ'.

Останній блок моделі - «ресурси, що захищаються» - не виконує самостійних функцій і може бути використаний для знищення запитів НСД (транзактів). Функції блоків спрощеної концептуальної моделі СЗІ показано у табл. 3.1.

Таблиця 1.

Функції логічних блоків СЗІ від НСД

№ блоку	Назва блоку	Функції
1	Порушник	Генерація запитів НСД з заданими інтенсивностями, які утворюють вхідний потік блоку «СЗІ».
2	Система захисту інформації, СЗІ	1. Імітація буфера (черги) запитів НСД. 2. Імітація обслуговування запитів НСД МЗ. 3. Розрідження вхідних і створення вихідних потоків пропущених і відсіяних запитів НСД.
3	Ресурси, що захищаються	Знищення запитів НСД (як відсіяних, так і пропущених МЗ СЗІ).

Таким чином, для побудови моделі СЗІ від НСД було використано наступні блоки:

- генератор транзактів - для імітації надходження запитів НСД;
- блок затримки - для імітації обробки МЗ запитів, що надходять НСД;
- черги - для імітації буфера запитів кожного з МОЗ;
- блоки знищення транзактів - для знищення запитів НСД (як пропущених, так і відсіяних МОЗ).

Таким чином, порушник в моделі представляється рядком генераторів транзактів (Рис. 3. 8), кожен з яких імітує надходження в систему НСД-запитів різних типів з відповідними інтенсивностями λ_i.

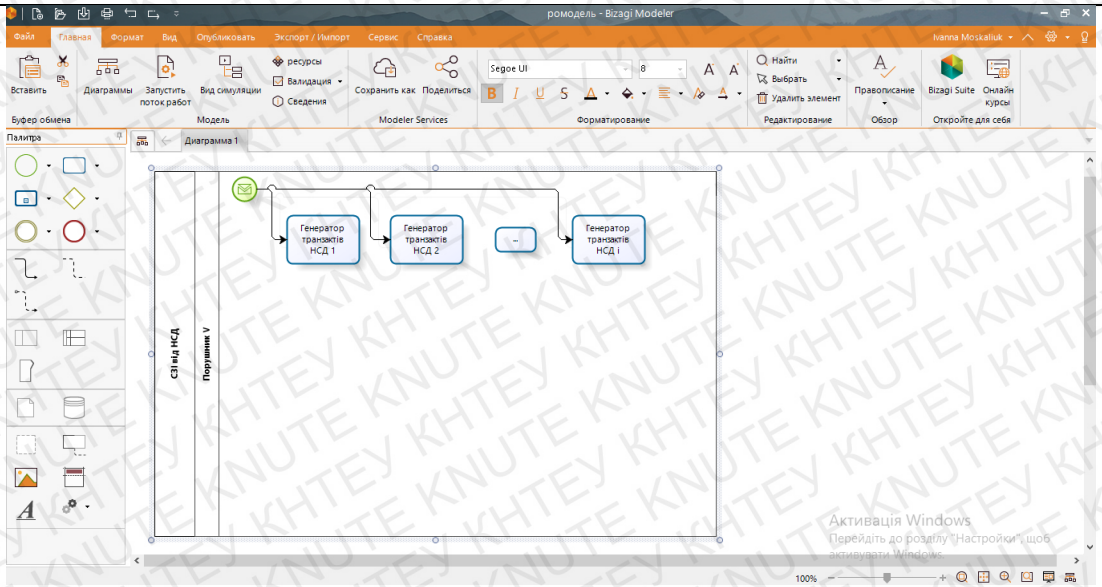

Рис. 3.8. Генератори транзактів

МЗ СЗІ від НСД складаються з трьох блоків:

- черги (буфери запитів на обслуговування) (Рис. 3.9)
- блоку очікування, що імітує обробку запиту НСД МОЗ (Рис. 3.10)
- умовного розгалуження, що імітує результат обробки (Рис. 3.11).

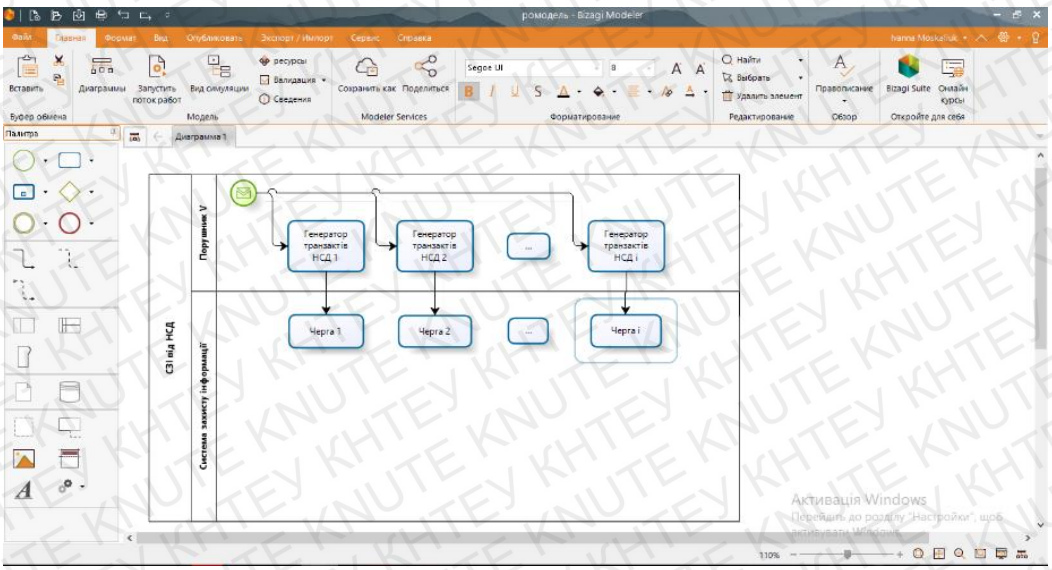

Рис. 3.9. Блоки черг

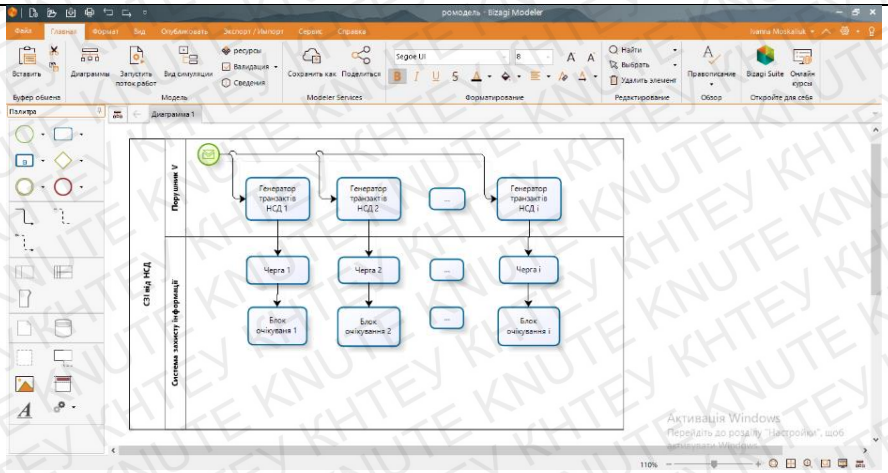

Рис. 3.10 Блоки очікування

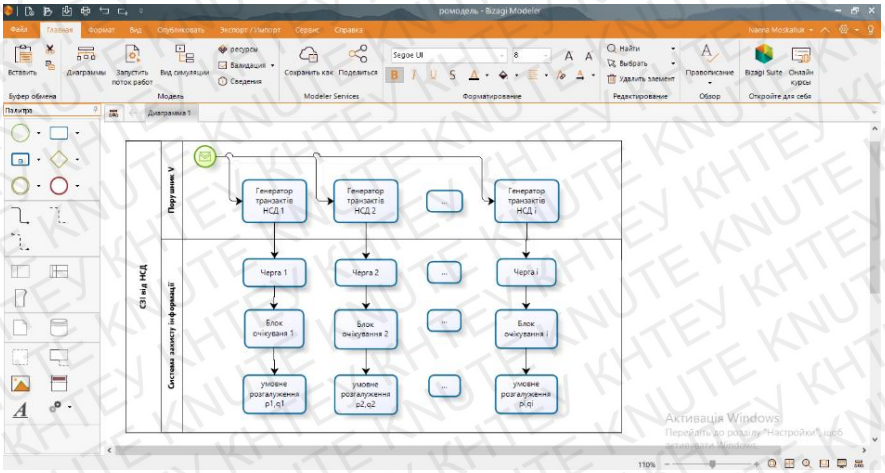

Рис. 3.11. Умовне розгалуження

Два блоки знищення транзактів (Рис. 3.12) служать для виведення транзактів з моделі.

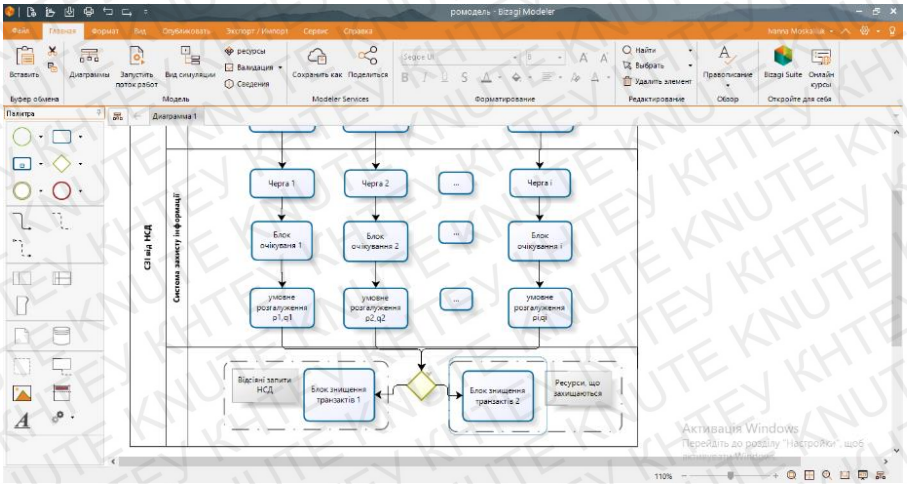

Рис. 3.12. Блоки знищення транзактів

Наявність цих блоків в моделі, зображеній на Рис. 3.13 є необхідною умовою її працездатності. На практиці апаратна і програмна складові СЗІ часто реалізуються у вигляді апаратно-програмного комплексу захисту даних (АПКЗІ) від несанкціонованого доступу. Апаратною частиною АПКЗІ може бути деякий контролер безпеки, пристрій криптографічного захисту даних, електронний замок і т.д.

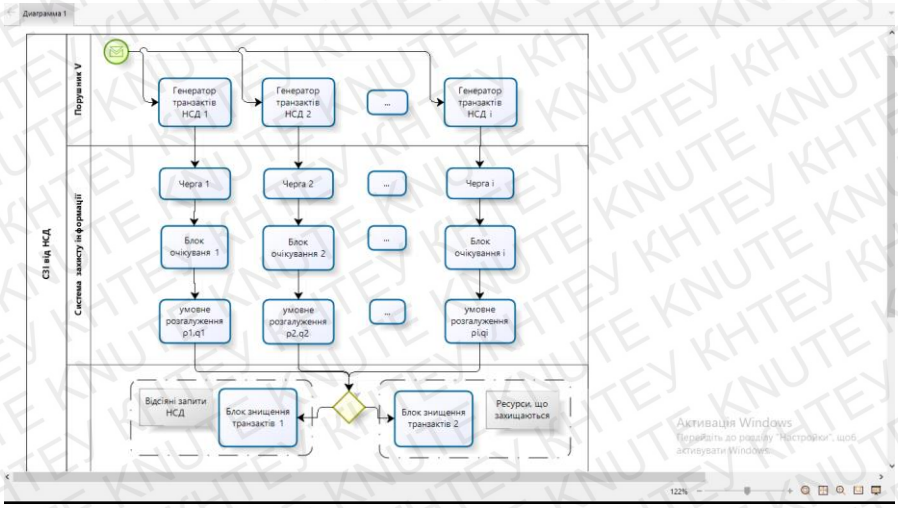

Рис. 3.13. Модель СЗІ від НСД

Апаратні засоби захисту реалізують додаткові МЗ даних і можуть функціонувати в постійній інформаційній взаємодії з програмною частиною (ядром) СЗІ. Виходячи зі сказаного, доцільним є облік в моделі СЗІ від НСД стану контролера безпеки і впливу змін його станів на процес захисту даних в АС.

Тому було створено відповідний блок моделі і описано його функціонування за допомогою діаграми станів (Рис. 3.14)

Рис. 3.14. Діаграма станів контролера безпеки

Модель СЗІ, що дозволяє враховувати вихід з ладу контролера безпеки, показана на Рис. 3.10.

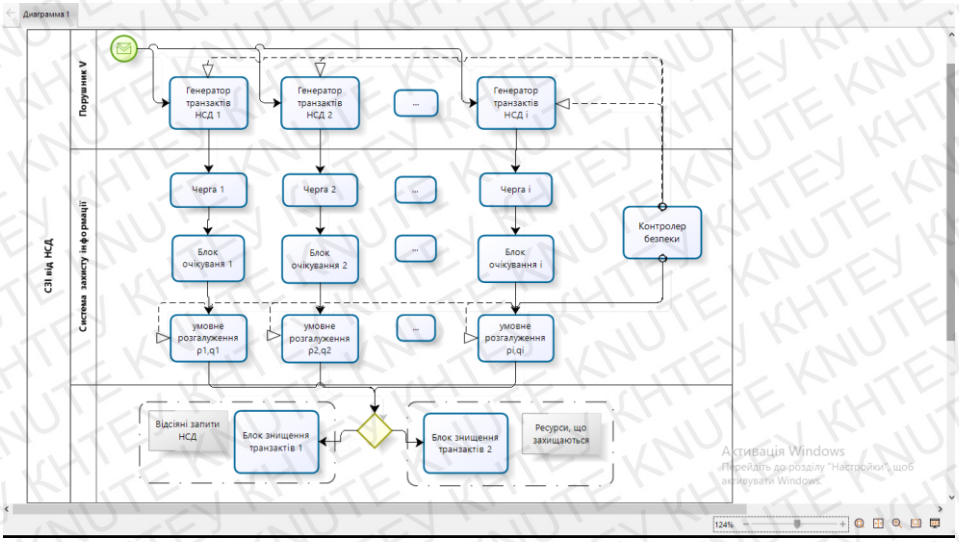

Рис. 3.10. Модель СЗІ від НСД

У модель додано блок «контролер безпеки». Пунктирні лінії, що зв'язують виходи цього блоку з генераторами транзактів і блоками умовних розгалужень, означають зміну станів контролера і виконання процедур, що впливають на відповідні блоки моделі.

ВИСНОВКИ

Основним завданням даного випускного кваліфікаційного проекту була розробка та програмна реалізація моделі захисту даних Digital Agency «Q-SEO»

В процесі написання випускного кваліфікаційного проекту було опрацьовано інформацію про захист даних, моделі захисту даних. На основі отриманої інформації був описаний оптимальний процес організації захисту даних на підприємстві за сукупністю і взаємозв'язку всіх видів і напрямків захисту даних, до яких належить організаційно-правовий, технічний, криптографічний та фізичний захист інформації(даних).

Застосування моделей, як спрощених описів важливих компонентів системи, дає змогу спростити розв'язок завдання створення адекватної реальним загрозам системи захисту.

Розглянуті у випускному кваліфікаційному проекті моделі використовуються для опису механізму захисту, аналізу системи захисту та систем дискреційного розмежування, контролю доступу, забезпечення цілісності даних, тощо.

У Draw.io розроблено концептуальну модель захисту даних підприємства від несанкціонованого доступу, яка в подальшому реалізована у BizAgi Modeler.

Модель буде використовуватись як складова загальної системи захисту даних Digital Agency «Q-SEO», що дозволить оптимізувати захист даних та зменшити кількість запитів НСД до даних підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк А.О. Моделювання систем захисту інформації: монографія. / А.О. Антонюк // Ірпінь: Національний університет ДПС України - 2015-273 с.
2. Вознюк А. Н., Кригер А. В., Тумуров Г. В. Модель организации защиты информации на предприятии / А. Н. Вознюк, А. В. Кригер, Г. В. Тимуров // Донецк – 2015
3. Гайтан О. М. Порівняльна характеристика програмних середовищ моделювання систем масового обслуговування / О. М. Гайтан // Полтавський національний технічний університет імені Юрія Кондратюка – 2015.
4. Голубенко О.Л. Політика інформаційної безпеки/ О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань, Ю.Є. Яремчук. – Луганськ: Вид-во СНІ ім. В. Даля. – 2009. – 300 с.
5. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. ДСТУ3396.0-96.
6. Дудикевич В.Б., Опірський І.Р. Аналіз моделей захисту інформації в інформаційних мережах держави / В.Б. Дудикевич, І.Р. Опірський // Системи обробки інформації – Л: Львів, Нац. ун-т «Львівська політехніка» - 2016 - № 4
7. Єжова Л.Ф. Управління інформаційною безпекою/ Л.Ф. Єжова, І.О. Мачалін, Я.В. Не-войт, В.О. Хорошко. – В2-х т. – К. : Вид-во ДУІКТ, 2011. – 236 с.
8. Загородников А. А., Козлов С. В. Модель защиты информации / А.А. Загородников, С. В. Козлов // / Харьков – 2014
9. Коленко В.В., Нарожний О.В., Сафонова Г.Ф.. Математичні моделі та методи процесів захисту інформації / В.В. Коленко, О.В. Нарожний, Г.Ф.

Сафонова // Інформаційні технології в освіті, науці та виробництві – О: Одеський нац. політех. ун-т. – с. 67-70

10. Кшнянкин А. П. Модель системы защиты информации на предприятии / А. П. Кшнянкин // Харьков – 2015 – с. 164-167
11. Мулеса О. Ю. Інформаційні системи та реляційні бази даних. Навч.посібник. – Електронне видання / О. Ю. Мулеса // Ужгород - 2018. – 118 с.
12. Опірський І.Р. «Класифікація моделей захисту інформації в інформаційних межах держави» // Науковий вісник НЛТУ України. – 2015. – с. 329-335.
13. Павлов І. М. Аналіз уразливостей систем захисту інформації / І. М. Павлов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – К: Київ - ВІТІ НТУУ "КПІ" – 2013 - №2(26)
14. Павлов І. М. Моделі життєвого циклу програмних механізмів захисту комплексної системи захисту інформації / І. М. Павлов // Сучасний захист інформації. –К.: 2011. − № 2. − С.60 − 68.
15. Смачило Т. В. Опорний конспект лекцій "Інформаційні системи та технології" / Т. В. Смачило // Тернопіль - 2012
16. Суприган О. І. «Основи організації захисту інформації» Навчальний посібник Вінниця ВНТУ 2012
17. Цымбалова А.А, Губенко Н.Е.Анализ модели использования ресурсов с точки зрения информационной безопасности. Информационные управляющие системы и компьютерный мониторинг — 2011 / Материали II всеукраинской научно-технической конференции студентов, аспирантов и молодых учёных. — Донецк, ДонНТУ — 2011, с. 292-295.
18. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.. Комплексні системи захисту інформації. Навчальний посібник – Вінниця : ВНТУ, 2017. – 120 с.

19. Корнеев Д.В. Обобщенная модель системы защиты ресурсов распределения вычислительной сети [Електроний ресурс] — Режим доступа к статье: Режим доступу до статті: URL: http://admin.smolensk.ru/virtual/expo/html/tesis.htm
20. Модели защиты информации [Електронний ресурс] - Режим доступу до статті: URL: https://studizba.com/lectures/10-informatika-i-programmirovanie/370-tehnologiya-postroeniya-zaschischennyh-informacionnyh-sistem/5013-15-modeli-zaschity-informacii.html
21. Сучасне розуміння поняття «інформація» [Електронний ресурс] - Режим доступу до статті: URL: http://5fan.ru/wievjob.php?id=41086
22. Основи інформаційних систем. [Електронний ресурс] - Режим доступу до статті: URL: https://pidruchniki.com/13170605/informatika/osnovi_informatsiynih_sistem