МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
Кафедра комп'ютеризованих систем управління

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

Олександр ЛИТВЕНЕНКО

"_____"_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ "МАГІСТР"

Тема: Програмна система для захисту даних клієнтів страхової компанії в банківській сфері.

Виконавець: Роман ПРИЙМАК
Керівник: Олена НЕЧИПОРУК
Нормоконтролер: Олена НЕЧИПОРУК

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп'ютерної та програмної інженерії

Кафедра комп'ютеризованих систем управління

Спеціальність 123 «Комп'ютерна інженерія»
(шифр, найменування)

Освітньо-професійна програма «Системне програмування»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Олександр ЛИТВЕНЕНКО
«_____»_____ 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
Приймака Романа Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи: «Програмна система для захисту даних клієнтів страхової компанії в банківській сфері.»

затверджена наказом ректора від «16» вересня 2022 р. № 1530/ст.

2. Термін виконання роботи: з 06.09. 2022 р. по 30.11.2022 р.

3. Вхідні дані до роботи: технічна документація, тестові дані, програмні продукти

4. Зміст пояснювальної записки:

Розділ 1 Дослідження предметної області;

Розділ 2 Особливості інформаційної безпеки банків;

Розділ 3 Проектування та розробка системи та методу збереження персональних даних для захисту даних клієнтів.

5. Перелік обов'язкового графічного (ілюстрованого) матеріалу:

1. Діяльність страхової компанії (контекстна діаграма);

2. Структурна схема розробленої системи;

3. Графічний інтерфейс програмного засобу;

4. Функціональний інтерфейс програмного засобу.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Постановка задачі та узгодження з дипломним керівником.	06.09.2022	Виконано
2	Формування структури розділів дипломної роботи	06.09.2022 – 08.09.2022	Виконано
3	Збір науково-технічного матеріалу до першої частини кваліфікаційної роботи.	08.09.2022– 13.09.2022	Виконано
4	Формування та оформлення першої частини кваліфікаційної роботи	13.09.2022 – 21.09.2022	Виконано
5	Збір науково-технічного матеріалу до другої частини кваліфікаційної роботи.	22.09.2022 – 28.09.2022	Виконано
6	Написання другого розділу кваліфікаційної роботи.	29.09.2022 – 08.10.2022	Виконано
7	Розробка практичної частини завдання до третього розділу кваліфікаційної роботи.	10.10.2022 – 23.10.2022	Виконано
8	Формування та оформлення третьої частини кваліфікаційної роботи.	24.10.2022 – 04.11.2022	Виконано
9	Оформлення пояснювальної записки.	07.11.2022 – 14.11.2022	Виконано
10	Оформлення графічного та ілюстративного матеріалу, підготовка до захисту кваліфікаційної роботи.	15.11.2022 – 24.11.2022	Виконано
11	Підписання необхідних документів.	21.11.2022	Виконано

7. Дата видачі завдання: «06» вересня 2022 р.

Керівник дипломної роботи _____ Олена НЕЧИПОРУК .
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Роман ПРИЙМАК.
(підпис студента) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Програмна система для захисту даних клієнтів страхової компанії в банківській сфері»: сторінок 80, рисунки 23, структурна схема 1, використаних джерел 10.

Об’єкт дослідження – захист даних клієнтів в банківській сфері.

Мета роботи – розробити програмну систему для захисту даних клієнтів страхової компанії.

Предмет – програмна система для захист даних клієнтів страхової компанії в банківській сфері.

Методи дослідження – розробка web- ресурсу з використанням мови програмування JavaScript. Побудова алгоритму захисту даних клієнта використовуючи лінійну алгебру та реалізовану на мові програмування Python. Побудова інформаційної моделі діяльності страхової компанії в концепції моделі IDEF в варіаціях AS-IS та TO-BE.

Практичне значення отриманих результатів – надання можливості захисту збереження даних клієнтів страхової компанії в банківській сфері.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 6
Вступ……7
Розділ 1 Дослідження предметної області 8
1.1 Поняття інформаційної безпеки 9
1.2 Безпека інформаційних систем страхових організацій 15
1.3 Методи захисту та збереження інформації 20
1.4 Висновки до розділу 27
Розділ 2 Особливості інформаційної безпеки банків 28
2.1 Людський фактор у забезпеченні інформаційної безпеки 29
2.2 Реалізація продуктів через банківський канал страховою компанією 35
2.3 Опис структури програмної системи 40
2.4 Висновки до розділу 42
Розділ 3 Проектування та розробка системи та методу збереження персональних даних для захисту даних клієнтів 43
3.1 Побудова інформаційної моделі діяльності страхової компанії 44
3.2 Розробка та реалізація методу захисту персональних даних клієнта 52
3.3 Опис розробленого програмного продукту 55
3.4 Засоби які використовувалися для розробки програмного засобу 69
3.5 Висновки до розділу 77
Висновки…… 78
СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ 80

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ISMS – система управління інформаційною безпекою;

FFA (force field analysis) – інструмент прийняття рішень який використовується для визначення важливості впливу перед запровадженням змін в бізнес процеси;

MFA – багатофакторна автентифіцікація;

2FA – двофакторна автентифікація;

EPDR – багаторівнева система захисту від взлому;

PCI DSS – стандарті безпеки, розроблений Visa, MasterCard, JCB, Discover і American Express;

СУІБ – система управління інформаційною безпекою.

Вступ

Актуальність теми – на сьогоднішній день в умовах сучасних реалій, функціонування систем захисту інформації осіб та їх кредитних страхових даних стало через звичайно актуальним процесом. Банки розуміють необхідність оновлення систем безпеки до найсучасніших, та важливість слідкування за тенденціями на ринку безпеки. Визначення найбільш підходящого способу захисту інформації для кожного конкретного випадку є залежить від великої кількості факторів, але максимальну ефективність можна досягти виключно застосовуючи комплексний підхід до вирішення проблем.

В сучасному інформаційному суспільстві захист персональних даних клієнтів банку – це вкрай важлива необхідність для успішного функціонування банку в конкурентному середовищі і роботи з клієнтами. Тому для успішного вирішення цього завдання банкам потрібно завжди бути в курсі останніх новинок захисту (як технічних, так і законодавчих) своїх даних і персональних даних своїх клієнтів, оскільки останнім часом атаки на банки для заволодіння базами даних стають все більш небезпечними.

Банківська інформація, в тому числі персональні дані клієнтів банку, є основним об’єктом оперування, тому вона вимагає належного захисту на законодавчому, технологічному та управлінському рівнях.

Перший розділ є теоретичним. В ньому подано стислу характеристику предметної області. Також приділено увагу особливостям предметної області, які впливають на організацію автоматизованої системи

В другому розділі описано сутність задачі, показано її роль і місце в діяльності банку, а також описано зв'язки даної задачі з іншими задачами і наведено схему інформаційної моделі задачі.

Третій розділ містить опис розробленої моделі з її подальшим описом, опис алгоритму захисту даних клієнтів та розробленого web-ресурсу.

Розділ 1 Дослідження предметної області

Ми всі оточені різними невизначеностями та ризиками в нашому житті. Будь то знаменитість чи звичайна людина; кожен живе в страху втратити цінні речі. Людей хвилюють різні проблеми, як-от проблеми зі здоров'ям, фінансові втрати в бізнесі, втрата смерті, незахищеність роботи тощо.

Отже, ми можемо сказати, що кожен відчуває ризики та невизначеність у певний момент свого життя.

Страхування пропонує спосіб забезпечити захист від різних фінансових втрат. Це вважається одним із засобів забезпечення не лише фінансової безпеки, але й емоційної та матеріалістичної безпеки.

Страхування підтримує, захищаючи нас від невизначених можливих ризиків, наприклад нещасного випадку, пожежі, раптової смерті, серйозних проблем зі здоров'ям, крадіжки зі зломом тощо. Страхування можна загалом класифікувати як страхування життя та загальне страхування.

- Страхування життя: це договір, який передбачає грошову

компенсацію в разі втрати працездатності або смерті людини. Навіть кілька полісів страхування життя складаються для забезпечення фінансової безпеки після виходу на пенсію або на фіксований період. Ми запозичуємо поліс страхування життя шляхом одноразової виплати або періодичних платежів, наприклад премії, суб'єкту, який надає страхування, тобто «Страховику або Страховій компанії».

Замість премії страховик або страхова компанія гарантує компенсацію гарантованої суми сім'ї у разі втрати працездатності, смерті або у визначений час.

- Загальне страхування: це договір, який забезпечує фінансове забезпечення у формі компенсації інших збитків, крім смерті. Ці фінансові втрати можуть бути пов’язані з різними зобов’язаннями, такими як подорожі, здоров’я, транспортний засіб, будинок тощо. Завдяки цьому страхові компанії зобов’язані виплатити гарантовану суму компенсації, яка покриває пошкодження автомобіля, фінансові втрати під час подорожі, медичні витрати під час лікування у зв’язку зі здоров’ям, фінансовими втратами через пожежу, крадіжку чи стихійні лиха тощо. Загальне страхування в основному складається з 5 типів, тобто медичне страхування, страхування транспортних засобів, страхування подорожей, страхування житла та страхування від пожежі.

Страховий бізнес заснований на роботі з невизначеністю. Таким чином, страховику необхідно враховувати широкий спектр можливих ризиків і результатів, які можуть вплинути на поточний і майбутній фінансовий стан.

1.1 Поняття інформаційної безпеки

Для забезпечення безпечної передачі необхідно визначити основні напрями захисту. Комерційна таємниця - це інформація захищена від несанкціонованого вторгнення, або крадіжка інформації.

Комерційна інформація може бути цікавою конкурентам підприємства. Наприклад, фінансова звітність, сума грошей на рахунках, список ділових партнерів, обіг коштів, укладати контракти тощо. Широко використовуються засоби прихованого спостереження та прослуховування у комерційній діяльності в галузі безпеки та життя окремих осіб.

Для забезпечення безпеки інформації шляхом створення служби безпеки або скористатись послугами охоронних компаній, які мають досвід роботи в галузі інформаційної безпеки. На додаток до організаційних заходів захисту інформації від несанкціонованого доступу, не слід нехтувати технічними засобами.[9]

Основними виробниками спеціального обладнання є США, Німеччина, Японія. Є зразки побутової техніки. Комерційні фірми вже пропонують ці продукти у широкому асортименті. .

Є багато технічних інформаційних каналів. Технічні канали витікання інформації може бути природними і штучними. Природні канали включають акустичний канал; телефонні лінії; радіолінія (радіотелефон, пейджинг, радіостанції тощо); офісне обладнання паразитні викиди.

Природні канали можуть контролюватись, наприклад, за допомогою записуючих пристроїв.

Штучні канали створюються навмисно. Голосові дані можуть бути записані або передаватися за допомогою радіохвиль (мініатюрні передавачі) та стаціонарні телефони (лінії сигналізації, блок живлення). Будь-який провідник лінія може використовуватися передачі сигналів як провідника чи антени. Отже, можна підключити передавачі нескінченно.

Захист даних може бути активним та пасивним. Активний захист є причиною виведення шкідливих перешкод інформації. Пасивний спосіб – визначає канали інформації.

При виборі пристроїв для захисту інформації необхідно проконсультуватися з фахівцями. Вони допоможуть вибрати правильне обладнання, щоб задовольнити вимоги.

Захист від несанкціонованого доступу до комп'ютерної інформації набуває все більшого значення. Виникнення локальних та глобальних комп'ютерних мереж, електронної пошти, обміну інформацією та програмних продуктів призвело до можливості несанкціонованого доступу для захисту інформаційних систем банків, страхових компаній, викрадення негрошових активів та комерційної таємниці.

Шифрованого факсимільного зв'язку та комп'ютерної інформації призначені для захисту даних, що передаються каналами зв'язку. При передачі інформації з одного пункту на інший відбувається шифрування і дешифрування на стороні, що приймає. Зашифрована швидкість передачі даних, наприклад, за допомогою кодерів компанії AT&T становить від 20 кбіт/с до 2 Мбіт/с.

Найбільш поширений метод захисту даних - використання відповідних програмних продуктів та пристроїв контролю доступу. Користувач може бути визнаний вихідним кодом на спеціальній картці, відбитків пальців і т.д.

Захист здійснюється даних з використанням різних програмних засобів. Вони включають програмне забезпечення, що забезпечує систему паролем, різні методи шифрування, копія програмного забезпечення захисту продуктів і поширення вірусів. Широкий спектр існуючих апаратних та програмних засобів дозволяє: ідентифікувати користувача.

Також можливо обмежити повноваження для доступу до пристроїв і розрізняти роботи за часом; обмежити доступ до банків даних;

- використовувати систему паролів; вести облік користувальницького досвіду та спроб несанкціонованого доступу;
- забезпечують налаштування програмного середовища залежно від прав користувача;
- для захисту конфіденційності, цілісності та достовірності інформації, що передається каналами зв'язку.

Як правило, під час промислового шпигунства не так оприлюднили факти злому інформації. Найбільш поширені випадки - запис розмови, і магнітофони, прослуховування та радіомікрофони. Для підйому комерційної інформації з бездротових мікрофонів, реєстратори, контролери, телефонні лінії, невеликі телевізійні камери тощо.

Наприклад, управління телефонної лінії, ви можете отримати повну інформацію про звички абонента, його зв'язок, діяльність та повсякденне життя. У випадку звичайного радіотелефону, це завдання спрощується, тому що лінія достатньо, щоб слухати за допомогою звичайного приймача, що сканує.

Під системністю як основною частиною системно-концептуального походу розуміється:

- системність цільова, тобто захищеність інформації сприймається як основна частина загального поняття якості інформації;
- просторова системність, що пропонує взаємопов'язане вирішення всіх питань захисту на всіх компонентах підприємства;
- системність тимчасова, що означає безперервність робіт із ЗІ, що здійснюються відповідно до планів;

- системність організаційна, що означає єдність організації всіх робіт з ЗІ та управління ними.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень та рішень, необхідних та достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт із ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи включає: передусім, вивчення об'єкта впроваджуваної системи; оцінку загроз безпеці об'єкта; аналіз коштів, якими оперуватимемо при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх та зовнішніх факторів; можливість додаткових змін у процесі побудови системи та повну організацію всього процесу від початку до кінця.

Комплексний (системний) підхід — це принцип розгляду проекту, у якому аналізується система загалом, а чи не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а чи не поліпшення ефективності окремих елементів. Це тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи доти, доки не визначено наступні її компоненти:

- Вхідні елементи. Це елементи, для обробки яких створюється система.
- Як вхідні елементи виступають види загроз безпеки, можливі на даному об'єкті;
- Ресурси. Це кошти, які забезпечують створення та функціонування
- системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри тощо). Зазвичай рекомендується чітко визначати види та допустиме споживання кожного виду ресурсу як у процесі створення системи, так і під час її експлуатації;
- Навколишнє середовище. Характерним прикладом важливості

вирішення цього завдання є розподіл функцій захисту інформації, що передається сигналами в кабельній лінії, що проходить по територіях різних об'єктів. Хоч би як встановлювалися межі системи, не можна ігнорувати її взаємодію Космосу з довкіллям, бо у разі прийняті рішення може бути безглуздими. Це справедливо як кордонів об'єкта, що захищається, так кордонів системи захисту;

- Призначення та функції. Для кожної системи має бути сформульована

мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи як її функція. Чим точніше і конкретніше зазначено призначення чи перелічені функції системи, то швидше і правильніше можна вибрати найкращий варіант її побудови.

Слід пам'ятати, що, зазвичай, глобальна мета досягається через досягнення множини менш загальних локальних цілей (підцілей). Побудова такого «дерева цілей» значно полегшує, прискорює та здешевлює процес створення системи;

Таким чином, враховуючи різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, цілі захисту можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу.

1.1.2 Основні аспекти обробки персональних даних клієнта та захист інформації при роботі з персональними даними.

Проблема термінологічного визначення та розуміння поняття «персональні дані» є однією із найскладніших при роботі в цій сфері. Саме у визначенні містяться межі та критерії віднесення тієї чи іншої інформації до цієї категорії. Аналізуючи ті визначення, які містяться в національних та міжнародних правових актах, слід зазначити, що в основному вони збігаються, цей термін визначається як: «будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною».

Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Ідентифікованою особа вважається, якщо її можна безпомилково виділити

серед інших. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи). Однак, за певних умов наявність меншої кількості інформації чи певного об'єму іншої інформації є достатніми для того, щоб ідентифікувати особу.

1.1.1.2 Поняття обробки персональних даних

Обробка персональних даних – це «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем».

Всупереч поширеному помилковому твердженню обробкою є не лише вчинення вказаних дій із систематизованою сукупністю персональних даних (базою даних, реєстром, каталогом, досьє тощо). Збір, реєстрація, накопичення чи будь-яка інша дія з боку володільця інформації навіть про одного суб'єкта персональних даних, у будь якій формі є обробкою відповідно до положень Закону.

Серед інших термінів, пов'язаних із обробкою, слід виділити також «знеособлення персональних даних». Під знеособленням розуміємо вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу. Вказане положення необов'язково передбачає повне видалення будь-яких даних, що дають можливість ідентифікувати суб'єкта (хоч така операція і охоплюється терміном знеособлення). Натомість мова йде скоріше про вжиття заходів, спрямованих на унеможливлення ідентифікації суб'єктів володільцем, у чиєму розпорядженні перебувають їх персональні дані/працівниками, що використовують ці дані.

1.1.2.2 Поняття захисту персональних даних:

Поняття захисту персональних даних є доволі широким та зазвичай включає два ключових елемента. Перш за все, це зобов'язання володільця вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

По-друге, це зобов'язання кожного працівника володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, так зване зобов'язання конфіденційності. [10]

Перед отриманням доступу до персональних даних кожен працівник повинен пройти процедуру ідентифікації/автентифікації, зокрема шляхом особистого введення індивідуального та відомого лише йому паролю (чи іншим способом, наприклад шляхом використання індивідуальної картки з вбудованою мікросхемою, яка автоматичну запускає визначені для конкретного користувача налаштування та ін.).

Це повинно забезпечити, що лише визначений працівник зможе працювати за певним робочим місцем чи за будь яким робочим місцем, однак із визначеними особисто для нього налаштуваннями доступу до персональних даних. Окрім цього, це дасть змогу ідентифікувати працівників, які працюють в системі, за допомогою присвоєного ними ідентифікатора.

1.2 Безпека інформаційних систем страхових організацій

Запровадження інтелектуальних інформаційних систем у страховому секторі створює багато перешкод і викликів. Занепокоєння щодо безпеки та конфіденційності конфіденційної інформації зростає з кожним роком через кілька тенденцій, таких як бездротові мережі, обмін інформацією про здоров'я та особисту інформацію, а також хмарні обчислення.

Коли говорити про безпеку, автентифікація є дуже важливою. Автентифікація неправильно розуміється як акт встановлення або підтвердження того, що твердження, зроблені суб'єктом або про нього, є правдивими. Він виконує життєво важливу функцію в будь-якій страховій організації в багатьох сферах, наприклад, забезпечує доступ до корпоративних мереж, захищає особистість інших користувачів і гарантує, що користувач є тим, ким він або вона себе видає.

Найбільш очевидні проблеми під час використання розумних інформаційних систем стосуються конфіденційності. Наприклад, якщо штучний інтелект здатний визначити, що хтось має певний розлад або хворобу, порівнюючи публічну інформацію, отриману з соціальних мереж або публічних джерел, можна навести аргумент, що це є порушенням прав на конфіденційність або є щонайменше, етично сумнівно. Штучний інтелект використовує не лише загальнодоступну інформацію про клієнта, але й його особисту інформацію, що викликає занепокоєння щодо захисту даних.

Дані можуть бути відсутні, пошкоджені, суперечливі або не стандартизовані (наприклад, частини інформації, записані в різних форматах у різних джерелах даних), і не мають стандартного словника.

Проблеми з даними в охороні здоров'я часто сприймаються як результат обсягу, складності та неоднорідності даних, їх поганої математичної характеристики та неканонічної форми.

Коли дані не є статистично обґрунтованими, вони знижують їхню ефективність для навчання. У результаті штучний інтелект може зробити багато помилкових припущень у страховому секторі, що в кінцевому підсумку може стати дискримінаційним (наприклад, зробити страхування дорожчим для меншин).

Достовірність результатів прийняття рішень на основі ШІ у страховому секторі також може бути під сумнівом. Відомий афоризм про те, що кореляція не є причинно-наслідковим зв'язком (це означає, що не завжди статистична ймовірність відображає справжню причину), справедливий тут, як і всюди.

Крім того, деякі характеристики, які корелюють із підвищеним ризиком або підозрою в шахрайстві, можуть бути оскаржені як дискримінаційні, якщо немає явного причинно-наслідкового зв’язку між характеристикою та ризиком підозри.

1.2.1 Побудова систем безпеки

Якщо є платформа, яка об’єднує систему охоронної сигналізації, систему моніторингу, систему пожежної сигналізації та інші системи, це найкращий спосіб забезпечити безпеку банку.

Система моніторингу мережевої сигналізації є хорошим рішенням, яке допоможе відділу безпеки банку впоратися з подіями безпеки. Він об’єднує систему охоронної сигналізації та систему моніторингу в одне рішення. Він об’єднує раніше розділені системи охоронної сигналізації та системи моніторингу (CCTV) в одну платформу. Рішення має багато потужних функцій:

- Функція перевірки зловмисників: перевірка сигналів тривоги за допомогою відео в реальному часі, коли відбувається подія. Відео в реальному часі може з’являтися автоматично та записуватися, коли спрацьовує сигналізація на панелі керування. Завдяки цій високоякісній системі моніторингу мережевої сигналізації на основі IP користувачі можуть дивитися відео в реальному часі, щоб вперше знати, що насправді відбувається.
- Функція збереження відео: Відеозапис тривожного моменту транслюватиметься та безпечно зберігатиметься на сервері платформи. Записане відео можна переглянути в будь-який час. Він надає високоякісні відеозаписи як докази, що полегшує затримання підозрюваного зловмисника та відшкодування збитків.
- Функція карти: карта може автоматично спливати, коли відбувається подія.
- Дистанційне керування: користувачі можуть дистанційно ставити, знімати з охорони та контролювати контрольні панелі сигналізації в центрі моніторингу сигналізації.
- Швидше прийняття рішень**:** надсилаючи живе відео в режимі реального часу,

система дозволяє користувачам негайно перевірити спрацьовування тривоги. У свою чергу, це дає змогу швидко відправляти групу реагування або екстрені служби на місце події, якщо це необхідно.

1.2.2 Організаційні засоби щодо захисту інформації

Багато в чому банківські та страхові оператори, мабуть, найбільше вразливі до кіберзлочинності порівняно з будь-яким іншим типом компаній. Вони не тільки оперують великими сумами грошей, але й відповідають за фінанси своїх клієнтів.

Розглянемо 4 основних фактори для збереження даних клієнтів:

1) Багатофакторна автентифікація (MFA)

Три ключові ідентифікатори, які можна використовувати для сильної стратегії MFA:

- Те, що користувач знає (секретний пароль);
- Щось, що є у користувача (банківський токен, який генерує код, його телефон тощо);
- Щось, ким є користувач (біометричний фактор, наприклад його відбиток пальця, сканування сітківки ока або голос).

Зазвичай експерти почуваються впевнено, покладаючись лише на два з них для надійної 2FA (двофакторної автентифікації), але ще безпечніше з усіма трьома. Зауважте, що жодна з цих типів інформації не є незламною – навіть біометричні дані можуть бути підроблені зловмисниками, що часто має руйнівні наслідки.

2) Керування привілейованим доступом

Важливо переконатися, що зловмисники не можуть використати привілейовані облікові записи у вашій IT-екосистемі, оскільки це може відкрити для них всю вашу цифрову діяльність. Щоб негайно усунути критичні вразливості, видаліть права адміністратора з усієї вашої організації та почніть використовувати надійне рішення для керування привілейованим доступом, щоб захистити свою робочу силу.

3) Захист мережі

Не тільки ваші кінцеві точки потребують надійного захисту. Ваша периметральна мережа також вразлива до атак з боку зловмисників або будь-кого, хто знаходиться поблизу офісу. Заходи банківської та страхової кібербезпеки не можуть ігнорувати точки входу в периметр, оскільки так багато людей відвідують банки щодня. (Більш детально про цей параметр в розділі 1.3.2).

4) Стратегія багаторівневої оборони або EPDR

Потужний захист складається з кількох рівнів , призначених для вирішення та усунення всіх можливих точок входу для зловмисників. EDR (Endpoint Detection and Response) давно вважається золотим стандартом кібербезпеки, але наша власна вдосконалена версія Endpoint Prevention, Detection and Response дійсно надає все необхідне, щоб бути на крок попереду зловмисників.

1.2.3 Порівняння існуючих стандартів систем захисту банківських даних

Існують три основні міжнародні стандарти безпеки банківської діяльності для фінансових установ:

- PCI DSS;
- ISO/IEC 27001;
- SWIFT CSP.

Розглянемо кожен з них більш детально:

Стандарт безпеки даних індустрії платіжних карток (PCI DSS) — це набір стандартів безпеки, розроблений Visa, MasterCard, JCB, Discover і American Express у 2004 році. Програма безпеки, керована Радою стандартів безпеки індустрії платіжних карток (PCI SSC) , призначений для захисту онлайн- і офлайн-транзакцій кредитних і дебетових карток від крадіжки даних і шахрайства.

Хоча PCI SSC не має юридичних повноважень, очікується, що будь-яка компанія, яка виконує транзакції з кредитними або дебетовими картками, повинна відповідати стандарту PCI DSS. Сертифікація PCI вважається найбезпечнішим способом захисту конфіденційних даних та інформації, допомагаючи компаніям будувати довгострокові, засновані на довірі відносини зі своїми клієнтами.

ISO/IEC 27001 – це стандарт безпеки, який офіційно визначає систему управління інформаційною безпекою (СУІБ), призначену для забезпечення інформаційної безпеки під явним контролем управління. Як офіційну специфікацію він встановлює вимоги, які визначають порядок впровадження, контролю, підтримки та безперервного поліпшення СУІБ. Крім того, він наказує набір порад та рекомендацій, які включають вимоги до документації, зони поділу відповідальності, доступність, контроль доступу, безпека, аудит, а також коригувальні та профілактичні заходи. Сертифікація ISO/IEC 27001 допомагає організаціям дотримуватися багатьох нормативних та законодавчих вимог, пов'язаних з безпекою інформації.

Програма безпеки клієнтів (CSP) SWIFT допомагає фінансовим установам забезпечувати сучасний та ефективний захист від кібератак, щоб захистити цілісність ширшої фінансової мережі. Клієнти порівнюють заходи безпеки, які вони впровадили, з тими, що вказані в Customer Security Controls Framework (CSCF), перш ніж щорічно підтверджувати свій рівень відповідності.

Завдяки надійній сертифікації та показникам відповідності, CSP відображає спільноту дуже зацікавлених користувачів, які прагнуть зупинити кібератаки на своїх шляхах. Зі зміною середовища кіберзагроз змінюється і CSP.

1.3 Методи захисту та збереження інформації

Питання інформаційної безпеки стосуються безпеки системи (наприклад, захист цифрового збереження та мережевих систем/служб від впливу зовнішніх/внутрішніх загроз); безпека колекції (наприклад, захист вмісту від втрати або зміни, авторизація та аудит процесів сховища); а також правові та нормативні аспекти (наприклад, особиста або конфіденційна інформація в цифрових матеріалах, безпечний доступ, редагування).

Інформаційна безпека є складною та важливою темою для інформаційних систем загалом. Важливо покладатися на відповідний досвід у вашій організації та за її межами через урядові та інші мережі для загальних процедур інформаційної безпеки та порад.

Суворі процедури безпеки:

1. Забезпечити дотримання будь-яких законодавчих та нормативних вимог;
2. Захист цифрових матеріалів від ненавмисних або навмисних змін;
3. Забезпечення аудиторського сліду для задоволення вимог підзвітності;
4. Діяти як стримуючий фактор потенційних порушень внутрішньої безпеки;
5. Захист автентичності цифрових матеріалів;
6. Захист від крадіжки або втрати.

Багато типів цифрових матеріалів, відібраних для довгострокового зберігання, можуть містити конфіденційну та конфіденційну інформацію, яку необхідно захистити, щоб гарантувати, що до них не мають доступу неавторизовані користувачі.

У багатьох випадках це можуть бути юридичні чи нормативні зобов'язання організації. Цими матеріалами необхідно керувати відповідно до Політики інформаційної безпеки організації для захисту від порушень безпеки. ISO 27001 описує спосіб кодифікації та моніторингу процедур безпеки (ISO, 2013a). ISO 27002 надає вказівки щодо впровадження процедур безпеки, сумісних із ISO 27001 (ISO, 2013b). Відповідні організації можуть пройти зовнішню акредитацію та валідацію.

У деяких випадках Політика інформаційної безпеки вашої організації може також впливати на діяльність із збереження цифрових даних, і вам, можливо, знадобиться заручитися підтримкою ваших команд з управління інформацією та ІКТ, щоб полегшити ваші процеси.

Такі методи захисту інформації, як шифрування, ускладнюють процес збереження, і їх, якщо можливо, слід уникати для архівних копій. Тому для конфіденційних незашифрованих файлів може знадобитися більш суворе застосування інших підходів безпеки; це може включати обмеження доступу до заблокованих терміналів у контрольованих місцях (захищені кімнати) або жорсткі вимоги автентифікації користувача для віддаленого доступу.

Однак ці альтернативні підходи не завжди можуть бути достатніми або здійсненними. Шифрування також може бути присутнім у файлах, отриманих під час прийому від депонента, тому важливо знати про параметри захисту інформації, такі як шифрування, керування ключами шифрування та їхні наслідки для цифрового збереження. [4]

1.3.1 Інструменти організаційного захисту

Безпека інформаційних систем — це поєднання інформаційних активів і елементів керування, призначених для захисту компаній і організацій від нових загроз і вразливостей. Інформація будь-якої компанії захищена настільки, наскільки протоколи безпеки реалізовані для її захисту. Ненадійна інформація, що походить від неправильної політики безпеки, призводить до недовіри та невизначеності, що негативно впливає на безперервність діяльності суб'єкта господарювання.

Роль інформаційної безпеки полягає у встановленні політики, яка створює здорове робоче середовище та контролює процес обміну інформацією з кінцевою метою гарантування конфіденційності, доступності та цілісності. Найбільш очевидні виклики безпеці згруповані в криптографії, малих і середніх підприємствах, конфіденційності в хмарах, безпеці в Інтернеті, криміналістиці та показниках безпеки, серед іншого.

Об'єднання мереж або інформації щодо таких компаній є неприйнятним, оскільки це пов'язано із серйозними діловими, юридичними, суспільними та етичними наслідками.

Для того, щоб інформація була повністю захищена, кожен компонент інформаційної системи обробки повинен володіти деякими засобами контролю безпеки. Багатошаровість і накладання засобів контролю безпеки призводить до процесу, відомого як глибокий захист. Стратегія поглибленого захисту визначає захисні заходи, які застосовуються для захисту системи від загроз і вразливостей. Він визначає міцність безпеки інформаційної системи відносно найслабшої точки вразливості. Елементи керування можна використовувати для визначення механізму

побудови стратегії глибокого захисту. Використовувані типи засобів контролю включають адміністративний, логічний і фізичний.

1.3.2 Інструменти мережевого захисту

Ваша мережа стикається з загрозами будь-якої форми та розміру, тому має бути готова до захисту, ідентифікації та відповіді на повний спектр атак. Але реальність така, що найбільшу небезпеку для більшості компаній становлять не випадкові загрози, а скоріше добре фінансовані зловмисники, які націлені на конкретні організації з певних причин.

Нижче представлені 9 різних типів інструментів і методів мережевої безпеки:

- Контроль доступу:

Якщо зловмисники не можуть отримати доступ до вашої мережі, кількість збитків, які вони зможуть завдати, буде надзвичайно обмеженою. Але на додаток до запобігання несанкціонованому доступу, майте на увазі, що навіть *авторизовані* користувачі також можуть бути потенційною загрозою.

- Програмне забезпечення для захисту від зловмисного програмного забезпечення:

Зловмисне програмне забезпечення у формі вірусів, троянів, черв'яків, клавіатурних шпигунських програм тощо призначене для поширення через комп'ютерні системи та зараження мереж. Засоби захисту від зловмисного програмного забезпечення – це своєрідне програмне забезпечення безпеки мережі, призначене для виявлення небезпечних програм і запобігання їх розповсюдженню.

- Виявлення аномалій:

Механізми виявлення мережевих аномалій (ADE) дозволяють аналізувати вашу мережу, щоб у разі виникнення порушень ви отримували сповіщення про них досить швидко, щоб мати змогу реагувати.

- Запобігання втраті даних (DLP):

Часто найслабшою ланкою в безпеці мережі є людський фактор. Технології та політики DLP допомагають захистити персонал та інших користувачів від

неправомірного використання та, можливо, скомпроментованості конфіденційних даних або виходу цих даних з мережі.

- Безпека кінцевої точки:

Діловий світ дедалі частіше *використовує власні пристрої* (BYOD) до такого стану, коли різниця між персональними та бізнес-комп'ютерними пристроями майже не існує. На жаль, іноді персональні пристрої стають цілями, коли користувачі покладаються на них для доступу до бізнес-мереж. Безпека кінцевої точки додає рівень захисту між віддаленими пристроями та бізнес-мережами.

- Системи запобігання вторгненням:

Системи запобігання вторгненням (також звані виявленням вторгнень) постійно сканують і аналізують мережевий трафік/пакети, щоб можна було ідентифікувати різні типи атак і швидко реагувати на них. Ці системи часто зберігають базу даних відомих методів атак, щоб мати можливість негайно розпізнавати загрози.

- Сегментація мережі:

Існує багато видів мережевого трафіку, кожен з яких пов'язаний із різними ризиками безпеки. Сегментація мережі дозволяє надати правильний доступ до потрібного трафіку, одночасно обмежуючи трафік із підозрілих джерел.

- Інформація про безпеку та керування подіями (SIEM)

Іноді просто зібрати потрібну інформацію з такої кількості різних інструментів і ресурсів може бути надзвичайно складно, особливо коли час є проблемою. Інструменти та програмне забезпечення SIEM надають службам реагування дані, необхідні для швидкої дії.

- Інструменти безпеки віртуальної приватної мережі (VPN):

VPN із віддаленим доступом зазвичай використовують IPsec або Secure Sockets Layer (SSL) для автентифікації, створюючи зашифровану лінію для блокування інших сторін від прослуховування.

1.3.3 Інструменти мережевого захисту

Актуальність захисту обумовлюється наявністю великої кількості потенційних конкурентів, і навіть недоброзичливців, які можуть зашкодити компанії. Потрапивши у чужі руки, цінна інформація стає товаром. Її спотворення, псування чи плагіат можуть нашкодити репутації та фінансам компанії, завдати шкоди та сприяти виходу з ринку.

Основні види інженерно-технічного захисту інформації

Існує класифікація інженерно-технічного захисту інформації за видом, об'єктами впливу та технологіями. Виділяють такі види засобів інженерно-технічного захисту:

- Фізичні.

Використовуються з метою вирішення завдань з охорони підприємства, спостереження за територією та приміщеннями, здійснення контрольованого доступу до будівлі. До них відносять охоронно-пожежні системи, аварійне та локальне освітлення, а також охоронне телебачення. Фізичні засоби захисту інформації можна розділити на запобіжні, які виявляють і ліквідують загрози, які сьогодні використовують керівники багатьох підприємств.

- Апаратні.

До них відносяться електронні та механічні пристрої, призначені для інженерно-технічного захисту інформації та для протидії шпигунству. Їхнє головне завдання – виявлення каналів витоку інформації, їх локалізація (виявлення) та нейтралізація. Прикладами таких засобів можуть бути комплекси для пошуку мережних радіопередавачів, телефонних закладок та радіомікрофонів, що встановлюються з метою секретного прослуховування.

- Програмні.

Включають системи захисту інформації, що забезпечують захист секретних даних: проектів, креслень, стратегічних і тактичних завдань фірми, фінансових і бухгалтерських даних, відомостей про працюючих співробітників.

- Криптографічні.

Спеціальні системи шифрування та кодування, що використовуються для захисту інформації при телефонних переговорах, робочих зустрічах, у рамках нарад. Принцип роботи криптографії полягає у застосуванні математичних моделей кодування повідомлень, що забезпечує ефективний захист інформації від несанкціонованої зміни та використання зловмисниками.

Завдяки технічним засобам, що забезпечують захист інформації, підприємство може не лише детально опрацювати та протестувати нові розробки та технології, а й встигнути запатентувати їх.

В процесі написання кваліфікаційної роботи були виконані наступні завдання:

1) Досліджено та проаналізовано предметну область;
2) Розглянуто поняття інформаційної безпеки та методів захисту та збереження даних;
3) Проаналізовано вплив людського фактору на забезпеченні безпеки інформаційної системи;
4) Розглянуто способи реалізації страхової продукції за допомогою банківської системи;
5) Описано структуру розробленої системи;
6) Побудовано та описано інформаційну систему на базі моделі IDEF;
7) Розроблено алгоритм захисту даних клієнтів;
8) Розроблено web-ресурс.

1.4 Висновки до розділу

В ході написання кваліфікаційної роботи, було досліджено поняття інформаційної безпеки та різні ви плаваючі з цього аспекти, було розглянуто безпеку інформаційних систем та елементи її захисту.

Інформаційна безпека має вирішальне значення в організації. Усю інформацію, що зберігається в організації, слід зберігати в безпеці. Інформаційна безпека буде визначена як захист даних від будь-яких вірусних загроз. Інформаційна безпека важлива в організації, оскільки вона може захистити конфіденційну інформацію, забезпечує роботу організації, а також забезпечує безпечну роботу додатків, реалізованих у системі інформаційних технологій організації, а інформація є активом для організації.

Навіть незважаючи на те, що інформація є важливою для організації, є кілька проблем, пов’язаних із захистом інформації та керування нею. Одним із викликів, з якими стикається організація, є відсутність розуміння важливості інформаційної безпеки.

Коли співробітникам бракує знань з інформаційної безпеки щодо збереження їх інформації, організація легко піддається атакам хакерів або інших загроз, які намагаються викрасти або отримати конфіденційну інформацію організації.

Розділ 2 Особливості інформаційної безпеки банків

Світова фінансова криза загострила проблеми страхового ринку України, а саме: низька фінансова надійність та платоспроможність страховиків; недостатні обсяги капіталізації та низька ліквідність активів страхових компаній; недостатній контроль і регламентація операцій з перестрахування; обмеження функцій Держфінпослуг щодо регулювання страхового ринку. Тому співпраця банків і страхових компаній є новим способом вирішення цих проблем.

Співпраця банків зі страховими компаніями є ефективним способом послаблення конкуренції за ресурси на фінансових ринках. Страхова компанія є дуже важливим партнером для банку, адже придбання полісу страхування ризиків є кроком до покращення роботи банківських установ та передачі ризиків страховій компанії. Концепція банківського страхування полягає у співпраці банків і страхових компаній для координації продажів, уніфікації страхових і банківських продуктів, каналів їх збуту або використання спільної клієнтської бази, а також доступу до внутрішніх фінансових ресурсів партнера. [5]

Термін «bancassurance» у перекладі з французької мови означає продаж страхових продуктів через мережу банківських відділень і дослівно перекладається як «банківське страхування» або скорочено «банківське страхування» (banque + assurance). Німецький аналог цього терміну – «allfinanz», який українські експерти трактують як «загальні фінанси». [2]

Під банківським страхуванням слід розуміти продаж страхових продуктів через мережу банків.

Проте є й інші розширені визначення банкострахування, як, наприклад, асортименту фінансових послуг, які можуть одночасно задовольнити як банківські,

так і страхові потреби клієнтів або залучення банківських установ у процес виробництва, маркетингу та збуту страхових продуктів.

Останніми роками простежується тенденція до універсалізації банківської діяльності, яка забезпечує надання банками всього спектру фінансових послуг. Поєднання банківських продуктів зручне для широких споживачів, бо забезпечує їм більший вибір послуг. Для банків це означає зростання продажів і встановлення тісних стосунків із клієнтом із звичайним наданням послуг.

2.1 Людський фактор у забезпеченні інформаційної безпеки

Система управління інформаційною безпекою (ISMS) сприяє створенню надійної системи безпеки та регулює систематичний спосіб використання ресурсів інформаційних технологій. Але технічний прогрес СУІБ не завжди гарантує безпеку загального організаційного середовища. Людський фактор змінює значну роль для інформаційної безпеки.

Таким чином, поведінка людини впливає на інформаційну безпеку та пов’язана з нею ризиками. У цьому розділі подано огляд наших досліджень з аналізу людського фактору та його впливу на ефективну систему управління інформаційною безпекою.

Дослідження вимагає аналізу силового поля для розуміння руйнівних і стрімких сил людських проблем і розглядають ці сили як цілі та перешкоди інформаційної безпеки. Тоді дослідження буде моделювати людські фактори,

одночасно намагаючись зрозуміти поточний час СУІБ в організації та її покращення з огляду на ідеальну тривалість. Він забезпечує заходи щодо інвестицій у фактори, які віддають цілям СУІБ.

Аналіз силового поля (FFA) широко використовується для управлінських змін в організаціях. Цю техніку розробив і запровадив Курт Левін (1947). Модель аналізу Левіна оцінює вплив усіх елементів і сил, які впливають на зміни. Ці фактори можна розділити на дві частини: руйнівні сили та стримувальні сили , як показано на рисунку 2.1

Рис. 2.1 Аналіз силового поля

Цей малюнок містить огляд FFA, в якому руйнівні сили протилежні сили перенавчання для досягнення ефективності цілі СУІБ.

Рушійні сили — це всі сили, які спонукають до змін і підтримують їх. Підтримка та повноваження вищого лідера є яскравим прикладом руйнівних сил. Навпаки, стримуючими силами є сили, які функціонують, щоб стримувати руйнівні сили та запобігати змінам, створюючи перешкоди та ризики.

Наприклад, занепокоєння щодо індивідуальних помилок може стати перешкодою для зміни мети стратегії СУІБ.

Посилення руйнівних сил при одночасному використанні стримуючих сил забезпечує послідовність цілей СУІБ, що запобігає ризикам шляхом забезпечення економічно ефективних заходів контролю. Людські фактори, що стосуються FFA, є дуже суб’єктивним питанням, яке потребує вимірювання для кількісної оцінки та

візуалізації. Для кожного цього фактора можна визначити чисельну шкалу впливу. Це кількісне визначення було результатом інтерв'ю, проведеного в нашому попередньому дослідженні у двох фінансових організаціях, у яких мали місце інциденти ІБ.

Аналіз силового поля (FFA) і ISMS широко зазначається, що людські діячі є суб'єктивними і потребують методів кількісного визначення. Використання аналізу силового поля (FFA) дозволяє скільки завгодно застосувати людський фактор, щоб допомогти вищому керівництву прийняти рішення щодо розподілу організаційних ресурсів для досягнення цілей СУІБ.

Ідентифікація руйнівних сил, які сприяють досягненню цілей ІБ і завдань організацій, слідуватиме за визначенням стримуючих сил. Сила шкірного крему буде розподілена за чисельною шкалою на основі відповідей, отриманих від людей, які взяли інтерв'ю в організації в нашому останньому дослідженні.

Ця числова шкала вимірює фактор впливу кожної сили. Зміна напряму СУІБ визначатиметься усуненням стримуючих сил і капіталізацією російських сил.

Ця цифра визначає статус обох сил і напрямків, у яких організація повинна рухатися для досягнення ефективного СУІБ. Моделювання цього зв'язку на основі аналізу силового поля вимагає, насамперед, розуміння та визначення поточного стану ISMS. Поточна ситуація перешкоджає позитивним змінам (перешкодам), щоб зупинити рух СУІБ до ідеальної ситуації (цілі), щоб зберегти статус-кво. Перешкоди сприяють ризикам, а цілі підвищують цілісність СУІБ.

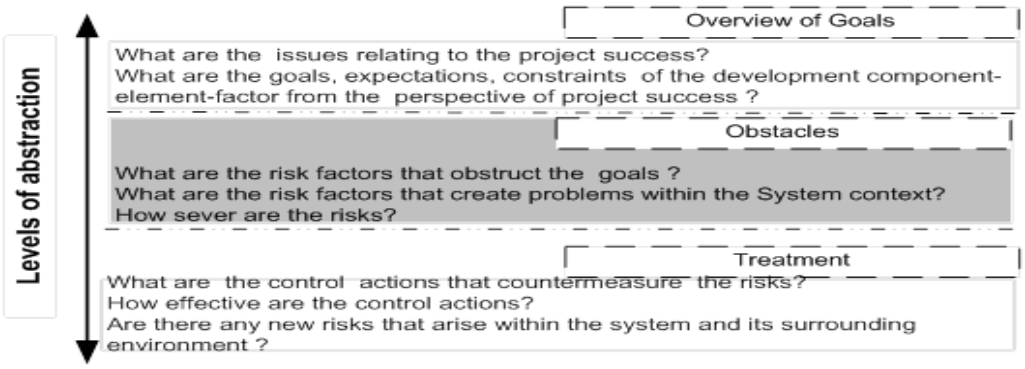

Рис. 2.2 Огляд рівнів моделі цілеспрямованого управління ризиками.

Цілеспрямована модель управління ризиками ефективно усуває ризики, які перешкоджають успішним результатам проекту. Цей підхід явно моделює зв’язки між цілями та факторами ризику, які перешкоджають цим цілям. Тоді оцінки є ризиками та вибираються відповідні контрольні заходи для пом’якшення ризиків, щоб проект міг досягти своїх цілей.

Цілі — це цілі, очікування та обмеження конкретного системного контексту та навколишнього середовища як директивні заяви про наміри, що забезпечують досягнення загального успіху проекту.

Ризики - це перешкоди, які мають наслідки, що підвищують ймовірність виникнення одиничних або кількох небажаних обставин, які перешкоджають досягненню цілей і, безумовно, знижують ймовірність успіху проекту.

Причина вибору мови цільового моделювання виникає в тому, що клітини та ризики є взаємодоповнюваними одиницями проекту програмного забезпечення. Ризик традиційний як заперечення однієї чи кількох цілей або втрата досягнення деяких відповідних цілей. Ризики завжди затьмарюються, і певні цілі можуть бути ризикованими.

Модель підтримує різні рівні абстракції від цілі до перешкоди і, нарешті, до лікування, як показано на малюнку 2.2 У верхній частині є цілі, тобто цілі, очікування та обмеження компонентів розробки.

Усередині містяться фактори ризику, які прямо чи опосередковано перешкоджають досягненню мети та викликають проблеми в контексті системи. У нижній частині знаходяться контрольні дії, які перешкоджають ризикам та їх наслідкам і сприяють досягненню цілей.

У запропонованій роботі зроблено спробу аналізу людських факторів у проактивний спосіб для ефективної системи управління інформаційною безпекою. Ми використовуємо комбінацію методу аналізу силового поля та цілеспрямованого моделювання ризиків управління для підтримки моделювання людських факторів. Мета конфлікту в тому, щоб зрозуміти, якою має бути ідеальна ситуація для організації, яка розглядає людські проблеми для загальних питань ІБ.

2.1.1 Загрози інформаційної безпеки банку з боку персоналу

Рушійні сили, які сприяють змінам у способах управління людськими факторами та пов’язані з ними, різноманітні, і їх надзвичайно важке застосування. Цілями в цьому документі є мета та вимоги, які необхідно ефективно вирішувати з урахуванням людських факторів, таких як помилки та апатія. У цьому розділі ми використали результати SWOT-аналізу для визначення руйнівних і стрімких сил для досягнення цілей СУІБ.

У цьому відношенні обізнаність, підтримка управління, бюджет і культура були визначені як руйнівні сили. Виходячи з обговорених інцидентів ІБ, ці фактори сприяли досягненню цілей СУІБ.

Деякі як прямі, так і непрямі людські фактори можна віднести до категорії рушійних сил. на те, що їх природа різна, вони можуть виступати за зміни в процесі проектування, впровадження та оцінки СУІБ, щоб бути ефективними та ефективними. Ці сили, однак, мають бути підтверджені та позитивними. Також необхідно змінити стан їх критичності.

Перешкодами в цьому дослідженні є стимулюючі сили, які перешкоджають змінам і, як наслідок, створюють ризики та нездатність системи досягти цілей. Наприклад, людський стрес не дозволяє людям прийняти зміни, які забезпечують ефективну роботу СУІБ. Люди в організаціях скептично ставляться до заходів і настанов СУІБ і можуть протистояти навчанню за допомогою нових принципів та процедур, які підвищують ефективність СУІБ.

Виявлення їхнього небажання та планування стратегії подолання цих перешкод є ключем до впровадження ефективної СУІБ в організації. Оскільки зміни стають все більш розширеним явищем у способі управління інформацією за допомогою технологій, розуміння людського фактору пропонує погляд на динамічну взаємодію між окремими особами та ISMS, щоб зрозуміти силу, що протистояти змінам.

На основі SWOT-аналізу деякі прямі та непрямі фактори були слабкими сторонами системи, які можна перевести на стимулюючі сили, що протистоять змінам у способах обробки СУІБ. Таким чином, силами опори є помилки, шлюбний

досвід, апатія, недбалість, стрес, спілкування та поява примусового застосування політики безпеки.

2.1.2 Кадрова політика з погляду інформаційної безпеки

Інциденти інформаційної безпеки зростають. Ці інциденти різним чином впливають на організацію. Найпоширеніші типи впливу на організацію, які необхідно виконати в профілі інформаційної безпеки: фінансові витрати, юридичні зобов'язання, діловий статус (репутація), крадіжка, вандалізм, пошкодження інтелектуальної власності, моральний стан і впевненість працівників і клієнтів.

Ці впливи, що перешкоджають системі під час опору, створюють перешкоди для змін, щоб зберегти поточний статус СУІБ недоторканим. Це відбувається тоді, коли руйнівні сили наполягають на змінах, щоб сприяти кращій та ідеальній ситуації, у якій ризики зменшуються та зменшуються.

Щоб пояснити час, ми використовуємо аналіз силового поля, який створює взаємодію двох конфліктуючих груп сил, тих, що намагаються сприяти змінам, руйнівних сил і тих, що хочуть зберегти-кво, що називається стримуючими статусами сил.

Щоб відбулися зміни, необхідно порушити рівновагу або поточний час, чого можна досягти за допомогою сприятливих умов для змін і усунення сил опори. На основі моделі FFA щоразу, коли руйнівні сили сильніші за стримувальні сили, статус-кво або рівноваги змінюються, і організації переходять від поточного статусу до кращого місця, яке ближче до ідеальної позиції системи.

Аналіз усіх сил показує, що необхідно підтримувати руйнівні сили, а рішення має прийняти команду вищого керівництва інформаційної безпеки для усунення стримуючих сил. Статус-кво або поточна ситуація СУІБ залишаються незмінними, після сили опору сильніші, ніж руйнівні сили змінюються. Це явно підтримує зусилля організацій від просування до цілого СУІБ, тобто кращої та безпечнішої ситуації.

У випадку зупинки в тій самій ситуації організації ризикують з ризиками, які збільшують вразливість і накопичують ризики. Керівник вищої ланки повинен вирішувати дуже важливі індивідуальні проблеми, як протистояння силам, таким як апатія, недбалість і стрес, забезпечуючи при цьому кращі засоби для покращення комунікації, політику забезпечення безпеки та мінімізуючи помилки шляхом запровадження навчальних програм.

Важливий аспект результату наголошує на індивідуальних характеристиках людських факторів як силу, що протистоять змінам. Високі бали отримали такі фактори, як апатія, помилка та стрес.

2.2 Реалізація продуктів через банківський канал страховою компанією

Банківське страхування — це нова концепція в секторі фінансових послуг, що означає використання банківських каналів дистрибуції для продажу страхових продуктів. Сенс банківського страхування полягає в тому, щоб поєднати виробничі можливості та продажі продуктів страхових компаній із дистриб'юторською мережею та великою сприйнятливою клієнтською базою банків. Це ситуація, коли страхові продукти пропонуються через канали розподілу банківських послуг разом із повним спектром банківських та інвестиційних продуктів і послуг. Банківське страхування намагається використати синергію між страховими компаніями та банками. [1]

Банки та страхові компанії є невід'ємною частиною фінансової системи однієї країни.

Співпраця між банками та страховими компаніями може здійснюватися в кількох формах, враховуючи той факт, що продукти, які вони пропонують, є взаємодоповнюючими.

Зростаючий фінансовий ринок, розвиток нових технологій, універсалізація банківської галузі та розширення небанківської діяльності призвели до швидкого розвитку нових каналів розповсюдження страхових продуктів через банки, що призвело до появи нової концепції під назвою «Банківське страхування». Це породило нову форму бізнесу та об'єднало всі їхні сили та зусилля для створення

нових продуктів для потенційних клієнтів. Зростання банку страхування залежить від того, наскільки добре банки та страхові компанії здатні долати операційні виклики, які виникають.

Банківське страхування просто означає продаж страхових продуктів банками. Банківське страхування використовується для опису партнерства або відносин між банком і страховою компанією, страхова компанія використовує банківський канал продажів для продажу страхових продуктів. [6]

У цій домовленості страхові компанії та банки об'єднуються, що дозволяє банкам продавати страхові продукти своїм клієнтам. Продаючи страхові поліси, банк заробляє а потік доходу, крім відсотків. Це називається гонорарним доходом.

Цей прибуток є суто безризиковим для банку, оскільки банк просто відіграє роль посередника для надання бізнесу страховій компанії. Страховики розглядають це як інструмент для збільшення проникнення та частки ринку, а банкіри використовують його для збільшення своїх комісійних доходів і згладжування нестабільності процентного доходу.

Банківське страхування – це пакет банківських і страхових послуг під одним дахом.

У різних країнах існують різні моделі банківського страхування, і деякі з них є такими наступне: [7]

1. Дистриб'юторські угоди – у найпростішій формі, що називається «зв'язаний агент», персонал банку продає продукти виключно одному страховику, або окремо, або в комплекті з банківськими продуктами.

2. Стратегічні альянси – це вищий ступінь втручання в розробку продуктів, надання послуг і управління каналами шляхом значних інвестицій банку в страховий бізнес без будь-яких умовних зобов'язань.

3. Спільне підприємство – йдеться про великий банк із добре розвиненою базою даних клієнтів, партнерами з великим страховиком і сильним досвідом роботи з продуктами та каналами для розробки нової потужної моделі дистрибуції. Крім того, банк і страхова компанія можуть домовитися про перехресні холдинги між собою для розподілу прибутку.

4. Група фінансових послуг – за умови подальшої інтеграції між банком і страховиком, страхова компанія може побудувати або купити банк, або банк може побудувати або купити страхову компанію.

2.2.1 Поняття страхування та управління ризиком

Співпраця та кооперація фінансових посередників у наданні фінансових послуг стає однією з основних характеристик сучасного економічного простору. Банківське страхування – це перспективна бізнес-модель, яка дозволяє страховим компаніям продавати свої продукти, канали збуту банків. Банки отримують вигоду, збагачуючи портфель клієнтів, а страховики мають доступ до баз даних клієнтів, профілів і клієнтів, таким чином мають можливість придбати більш широкий спектр продуктів і послуг для задоволення своїх вимогливих потреб.

Розширюються канали збуту фінансових продуктів і послуг, охоплюючи суміжні сектори фінансового ринку, що в свою чергу сприяє диверсифікації ризиків, зниженню операційних витрат, розширенню клієнтської бази.

Така співпраця набуває все більших масштабів. Це стає звичним явищем і відкриває нові перспективи для розвитку фінансової системи та її окремих підсистем.

Слід враховувати, що обидві фінансові установи повинні досягти згоди щодо певних організаційних, фінансових та управлінських питань для здійснення спільної діяльності.

На українському ринку банківське страхування знаходиться на початковому етапі розвитку. Переважаюча думка банків полягає в тому, що страхування є малоприбутковим бізнесом, і тому вони не зацікавлені в розвитку цього каналу продажів. Крім того, кінцеві користувачі все ще не виявляють особливого інтересу до різноманітних видів страхових продуктів, які пропонуються на ринку. Страхові компанії все ще орієнтовані на розвиток власних каналів продажів, і додатковим завданням для розвитку банківського страхування є програмні рішення для впровадження банківського страхування.

Керівництво більшості банків і страхових компаній, що працюють в Україні, усвідомлює переваги банківського страхування, тому інтенсивно працює над розвитком цього каналу дистрибуції. Ця діяльність особливо важлива в умовах світової економічної кризи, оскільки сприятиме більшому зростанню тих страховиків і банків, які пов'язані капіталом і контрактами в період після кризи.

2.2.1.1 Поняття, класифікація ризиків та їх оцінка

Страховий ризик означає ймовірність того, що щось піде не так, що призведе до фінансових втрат для вашого бізнесу або страховика. Бізнес-ризик і страховий ризик часто збігаються. Повністю розуміючи різні типи бізнес-ризику, ви зможете краще зрозуміти страховий ризик і, таким чином, як страхування може захистити ваш бізнес від серйозних проблем.

Ось чотири основні категорії ризику, які слід враховувати:

- Операційний: операційний ризик пов’язаний із повсякденною діяльністю вашого бізнесу, включаючи транспортне обладнання, співробітників, клієнтів і ваш загальний продукт або послугу. Страхуючи матеріальні активи, такі як обладнання та майно, ви можете зменшити ризики, а захищаючи свої бізнес-операції від зовнішніх подій, таких як стихійні лиха, ви будете захищені.
- Стратегія: Стратегічний ризик виникає, коли ваша бізнес-стратегія руйнується або узурпується вами чи іншими компаніями. Керуючи малим бізнесом, ви повинні розробити конкретну стратегію для свого продукту чи послуги та дотримуватися її. Якщо конкуренти підривають вашу стратегію, продаючи або знижуючи ціни на ваш продукт чи послугу, ви ризикуєте відстати у своїй галузі. Дуже важливо дослідити конкурентів і зрозуміти, як найкраще захистити стратегічні активи вашого бізнесу, наприклад інтелектуальну власність.
- Відповідність: Ризик невідповідності стосується здатності вашого бізнесу дотримуватися певних правил і норм, встановлених вашою галуззю чи урядом. Це включає такі речі, як податковий тягар, муніципальне зонування та закони про власність, закони про розподіл та інші правила та норми, пов’язані з вашим

бізнесом, наприклад HIPAA або належна виробнича практика. Щоб усунути ризик невідповідності, вам потрібно бути в курсі останніх нормативних актів у вашому секторі. Хоча ви не можете придбати страховку, пов’язану з податковими та іншими формами ризику недотримання, ви повинні знати про свої зобов’язання, розуміючи, за що може нести відповідальність ваш бізнес.

- Репутаційний: Останній тип ризику – репутаційний. Це означає захист вашого бізнесу від проблем безпеки, витоку даних та інших проблем кібербезпеки. Це також передбачає вживання заходів для захисту вашого бренду та логотипу. Ви можете застрахувати свій бізнес і дані клієнтів на випадок, якщо будь-яку з них буде скомпрометовано. [8]

2.2.1.2 Поняття та види страхування підприємницького ризику

Чистий або абсолютний ризик – це тип ризику, при якому немає прибутку для застрахованої особи або страхувальника. Цей ризик повністю поза контролем людини, і коли це має статися, він станеться. Для цих типів ризиків використовується термін неминучий. Це ризики, які підлягають страхуванню, і, відверто кажучи, страхування є єдиним способом пом’якшити наслідки завданої шкоди. Страхові компанії не несуть відповідальності за всі пошкодження. Натомість вони виплачують частину збитку застрахованій особі. [3]

Статичний ризик – цей ризик протилежний чистому ризику, і його можна уникнути за належного догляду. Відбувається це через недбалість страхувальника. Це також пов'язано з добровільними діями, які можуть завдати матеріальної чи фізичної шкоди людині в майбутньому. Ці добровільні дії можуть також включати образливі або кримінальні дії, вчинені особою. Ці типи ризиків також підлягають страхуванню, оскільки суму збитку можна легко визначити.

Специфічний або особистий ризик – це найбільш висвітлені види ризиків у страхуванні. Тут рішення однієї людини чи дія людини впливає на всю спільноту чи групу навколо неї. Це може бути через людську недбалість або через добровільне людське рішення. Однак люди відчувають втрату виключно через вибір чи помилку

іншої людини. Ці ризики підлягають страхуванню, оскільки вони захищають від невизначеного майбутнього лиха. Наприклад, через недбалість водія автобуса в ДТП може потрапити весь автобус.

Фундаментальний ризик – це неособисті ризики також називають фундаментальними ризиками. Вони не впливають лише на одну людину. Натомість це впливає на всю спільноту чи групу. Причиною можуть бути природні, соціальні чи політичні події. Ніхто не може уникнути цих ризиків, тому вони неминучі. Вони впливають на суспільство в більших масштабах із постійними наслідками. Наприклад, голод може вплинути на здоров'я всього суспільства. Вони підлягають страхуванню. Страховики надають страхувальникам необхідну суму до одужання.

Фінансовий ризик. Ці типи ризиків мають грошову оцінку, і страховики можуть розрахувати їх у грошовому еквіваленті. Тому вони підлягають страхуванню. Це загальні ризики, які неможливо передбачити, наприклад, втрата коштовностей, будь-яка крадіжка чи ДТП. Їх грошова вартість оцінюється відповідно до ринкової вартості, і страхувальник більш-менш погоджується з оціненою сумою. У разі смерті застрахованого кошти надаються його законним представникам.

2.3 Опис структури програмної системи

Система складається з наступних елементів (зображених на рисунку 2.1):

- Головної сторінки – котра являє собою основну сторінку web-ресурсу, на які розміщено основні напрямки та види страхування, та подано їх короткий опис, для більш детально ознайомлення з послугами необхідно перейти в розділ вибору типів страхування;
- Авторизації – даний елемент системи, дає можливість користувачу зайти через зареєстрований раніше ним аккаунт або за допомогою BankID (ресурс не зберігає банківські дані користувачів);
- Вибору типу страхування – після переходу в цей розділ користувач може ознайомитись з доступним переліком страхових послуг, які актуальні в даний момент. Цей розділ містить в собі 3 підпункти (автострахування, страхування

подорожей, та страхування від нещасних випадків), згідно цих підпунктів користувач вибирає необхідну йому послугу (або групу послуг) та додає їх в корзину для подальшої перевірки та оплати.

- Кошик – даний елемент системи відповідає за перегляд та зберігання вибраних користувачем послуг (або групи послуг), для перевірки перед наступним етапом (оплата), в випадку якщо його все влаштовує користувач переходе до наступного етапу.

- Вибір методу оплати – даний елемент системи являє собою останній пункт процесу вибору страхового полісу, після всіх етапів перевірки клієнт робить оплату за допомогою трьох доступних методів (розрахунок за допомогою банківського рахунку, розрахунок за допомогою отримання банківського кредиту та розрахунок банківською картою)

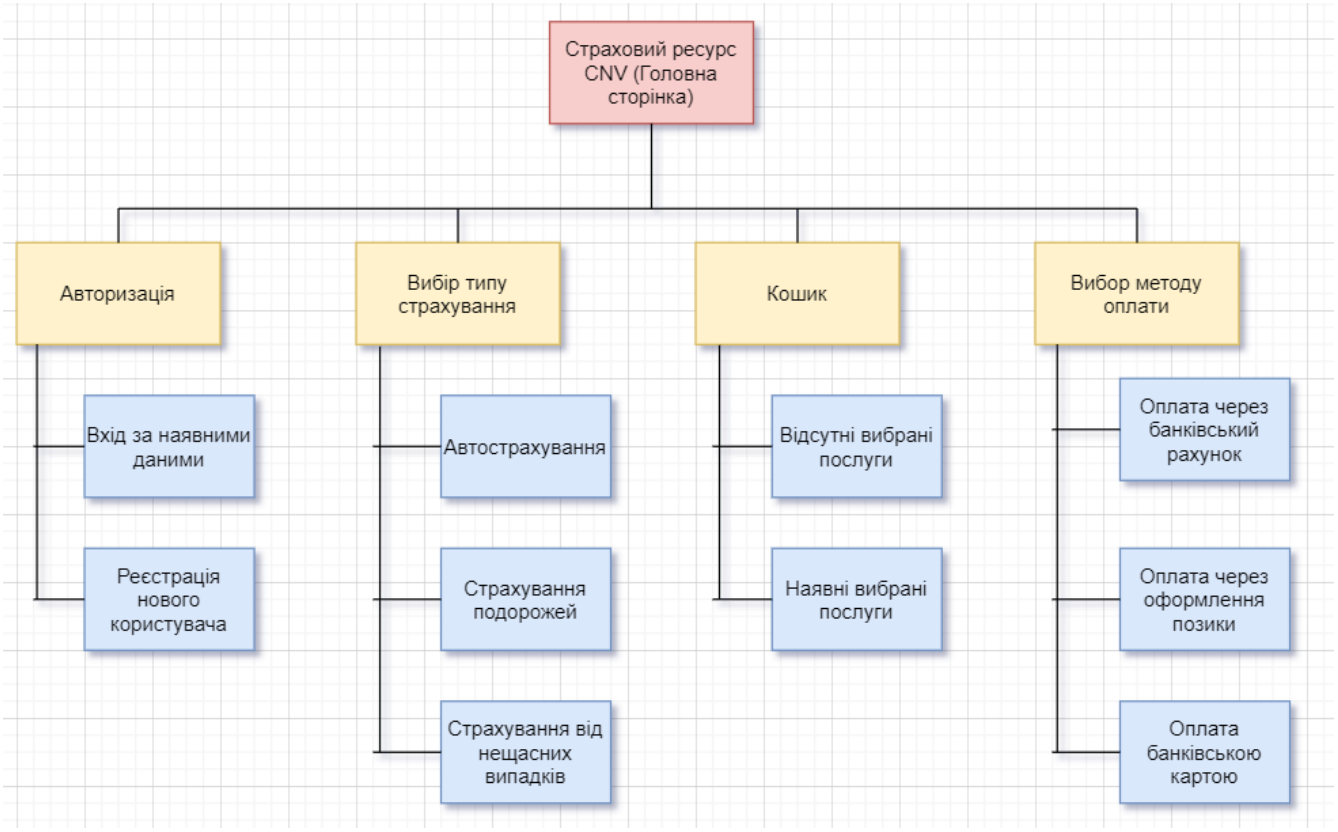

Рис. 2.1 Структура програмної системи

2.4 Висновки до розділу

В другому розділі кваліфікаційної роботи було розглянуто загрози інформаційним системам включаю людський фактор. Та розглянуто теоретично, можливість реалізації страхових систем в банківські.

Співпраця банків та страхових компаній є вигідною і для споживачів послуг останніх. Зазвичай, вигоди клієнтів проявляються в зручності при отриманні послуг, а також економії коштів та часу на їх оформлення. При цьому, недоліком банківського страхування може бути падіння довіри до банківської установи з боку тих клієнтів, які вважатимуть інтегровані продукти непотрібними чи нав’язливими.

Факт розголошення банком конфіденційних даних клієнтів, останніми також сприймається з недовірою. Успішність інтеграції в багатьох випадках залежить від здатності банка та страховика вчасно реагувати на загрози, які існують на фінансовому ринку і безпосереднім чином можуть вплинути на економічні інтереси фінансових посередників. Хоча сьогодні банки і страхові компанії працюють в складних умовах, але банківське страхування в Україні має досить великий потенціал для розвитку.

Розділ 3 Проектування та розробка системи та методу збереження персональних даних для захисту даних клієнтів

Страхування є системою захисту майнових інтересів громадян, організацій та держави, яка має стати необхідним елементом у світлі економічних, соціальних і політичних перетворень, що відбуваються в Україні.

Пріоритетними напрямками є банківське страхування, добровільне медичне страхування, а також страхування майна фізичних та юридичних осіб. Компанія надає послуги із сільськогосподарського, авіаційного страхування, страхування від нещасних випадків, іпотечного, туристичного страхування та інших видів страхування.

Головною метою організації страхової справи є забезпечення захисту майнових інтересів фізичних та юридичних осіб, які являються громадянами України.

Рентабельності страхової компанії забезпечують такі складові, як акумуляція коштів у страхових фондах та інвестування цих коштів у господарський обіг; задоволеність споживача послуг; мінімізація ризиків.

3.1 Побудова інформаційної моделі діяльності страхової компанії

Головною метою організації страхової справи є забезпечення захисту майнових інтересів фізичних та юридичних осіб, які являються громадянами України.

Рентабельності страхової компанії забезпечують такі складові, як акумуляція коштів у страхових фондах та інвестування цих коштів у господарський обіг; задоволеність споживача послуг; мінімізація ризиків. Графічний варіант цілей підприємства представлений на рис. 3.1.

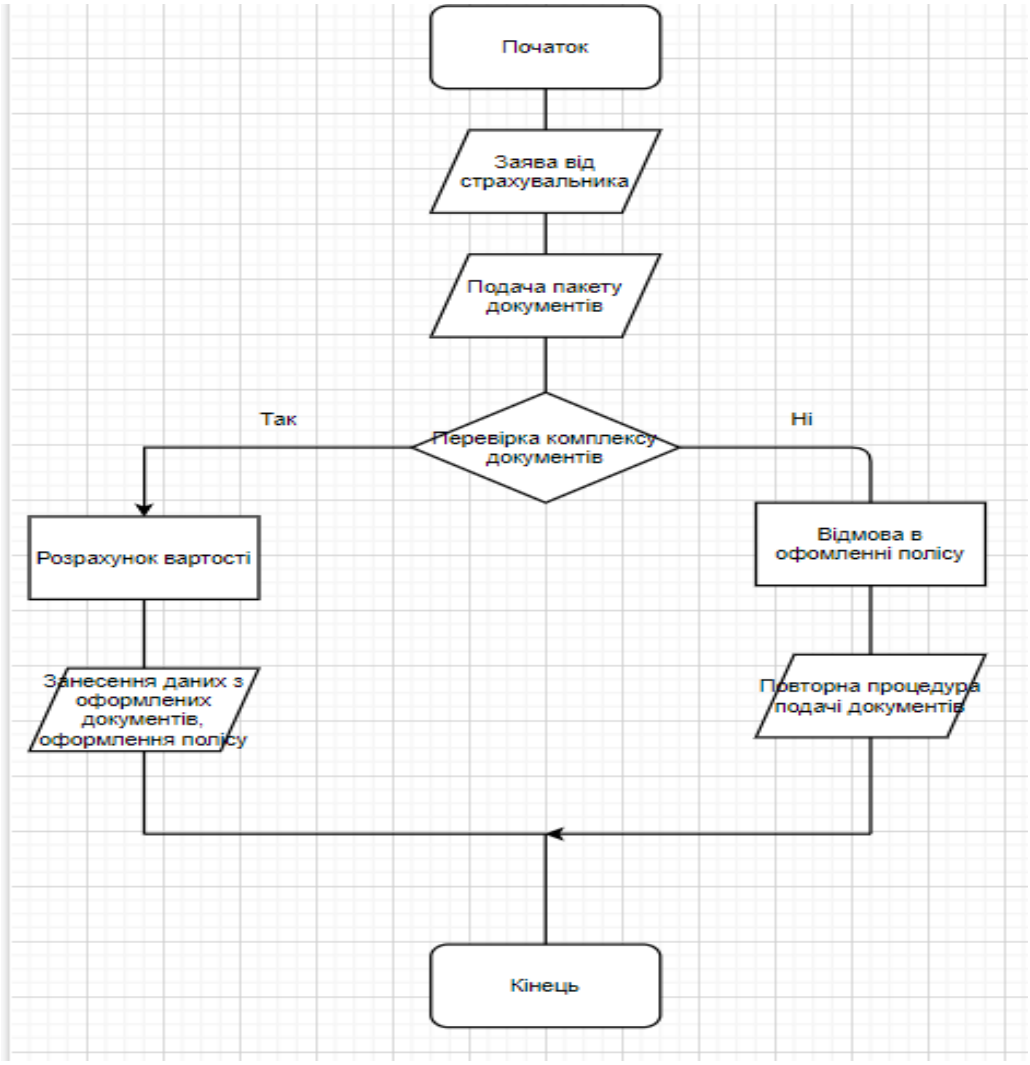

Рис. 3.1 Схема алгоритму розрахунку задач страхування.

Однією з основних цілей бізнес-моделювання є аналіз та вдосконалення діяльності організації чи підприємства. Не секрет, що продуктивність праці в Україні, яка визначається як валовий внутрішній продукт на одного зайнятого в

кілька разів менша за продуктивність праці в розвинених країнах. Іншими словами, ту саму роботу, яку в українських компаніях виконують кілька людей, у більш розвинених виконує один. Така ситуація визначається низьким рівнем застосовуваних українськими компаніями виробничих, інформаційних та управлінських технологій.

Однією з причин є недостатня організація праці. За оцінками фахівців впровадження українськими компаніями сучасних технологій організації та управління бізнесом зможе підвищити їхню продуктивність праці від півтора і вище разів. Для проведення аналізу та вдосконалення діяльності компанії необхідно побудувати та використовувати її бізнес-модель.

Бізнес-процес «Здійснення страхової діяльності» поєднує діяльність працівників відділів страхування, андеррайтингу. Сюди входить надання послуг із особистого страхування, майнового страхування, супроводження страхових договорів.

Підпроцес страхування майна включає у собі кілька подібних процесів, зокрема таких, як автострахування, страхування відповідальності й безпосередньо страхування майна фізичних і юридичних. Аналогічним чином, процес особистого страхування був сформований шляхом об'єднання процесів добровільного медичного страхування, страхування від нещасних випадків, страхування за кордон.

Підпроцес перестрахування об'єднав усі процеси, що описують заходи щодо передачі ризиків у перестрахування, з їх подальшим розподілом по інших компаніях. Цей підпроцес взаємодіє з партнерами і є крос-функціональним у межах підприємства – процес передачі ризиків від виду страхування змінюється не сильно.

Тепер коли основні бізнес-процеси компанії визначені, можемо перейти безпосередньо до їх моделювання.

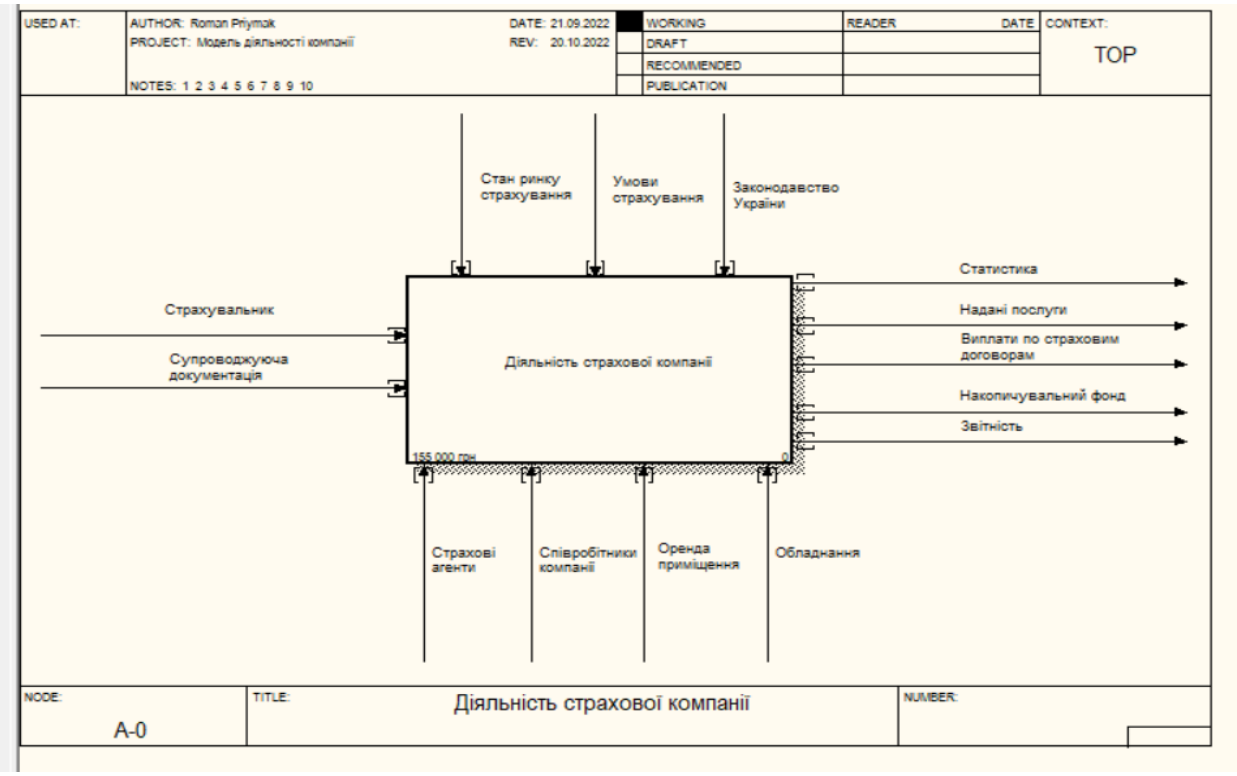

Рис. 3.2 Контекстна діаграмі діяльності страхової компанії.

На даній діаграмі бізнес-процесів страхової діяльності вхідною інформацією є: «Страхування» та «Супровідна документація».

Механізмами (ресурсами) є: "Страхові агенти, Співробітники компанії, Оренда приміщення та Обладнання"

Управлінням є: «Стан страхового ринку, Умови страхування та Законодавство України».

Виходами є: «Статистичні дані, Надані послуги, Виплати за договорами страхування при страхових випадках, сформований Накопичувальний фонд за рахунок збору страхових премій та Звітність».

При декомпозиції контекстної діаграми (Рис. 3.3) видно діяльність компанії, яка складається з: «Укладання страхового договору, Формування страхового фонду, фінансово-економічного аналізу страхової діяльності та Урегулювання збитків – відшкодування збитків при страховому випадку».

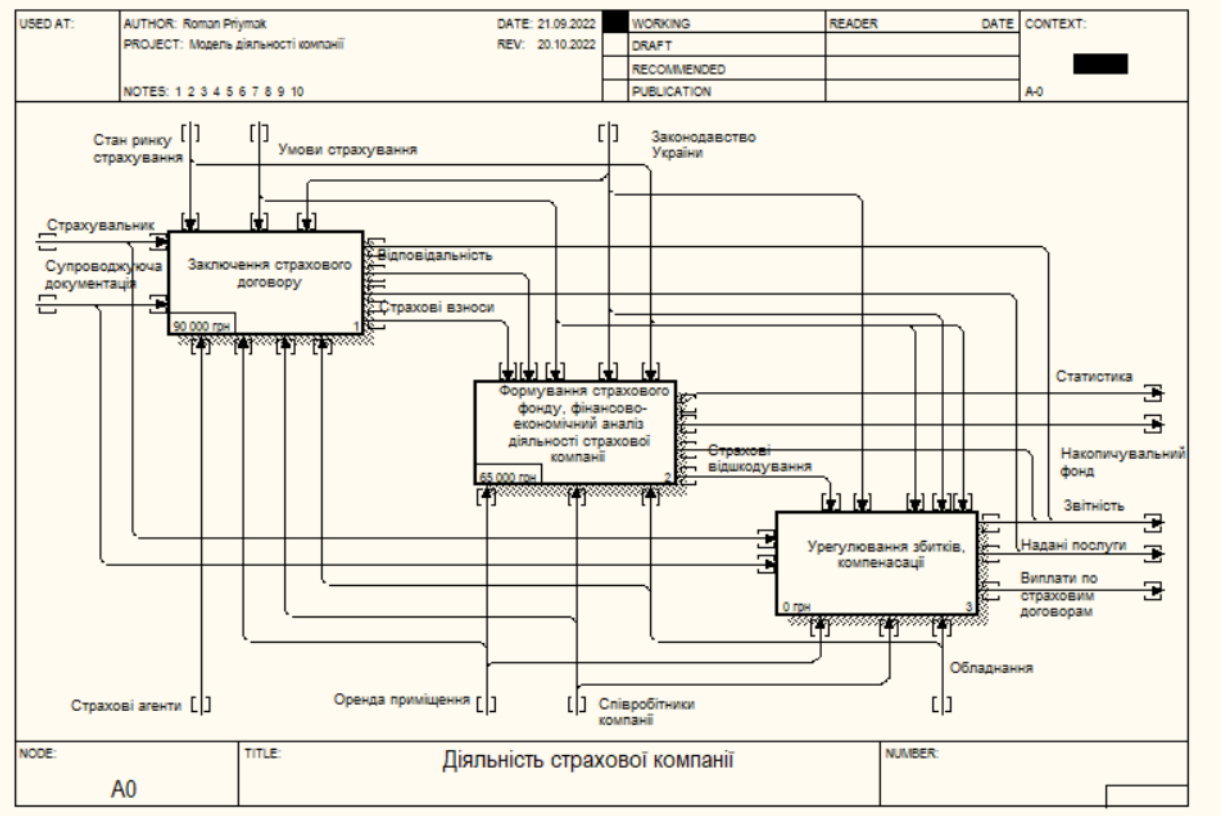

Рис. 3.3 Декомпозиція бізнес процесів діяльності страхової компанії.

У страховій компанії основною функцією є укладання страхового договору, за рахунок якого формується страховий фонд із отриманих страхових премій. Бізнес процес укладання страхового договору складається з: «Надходження замовлення від клієнта, оформлення страхового полісу та Видачі полісу страхувальнику» (Рис. 3.4).

Рис. 3.4 Діаграма бізнес процесу заключення страхового договору.

Основними складовими страхової компанії є оформлення страхового полісу та розрахунок страхової премії (Рис. 3.5).

На даній діаграмі бізнес-процесів вхідною інформацією є: «Отримання інформації від клієнта: дані про автомобіль, власника, осіб допущених до управління, термін страхування, період використання транспортного засобу».

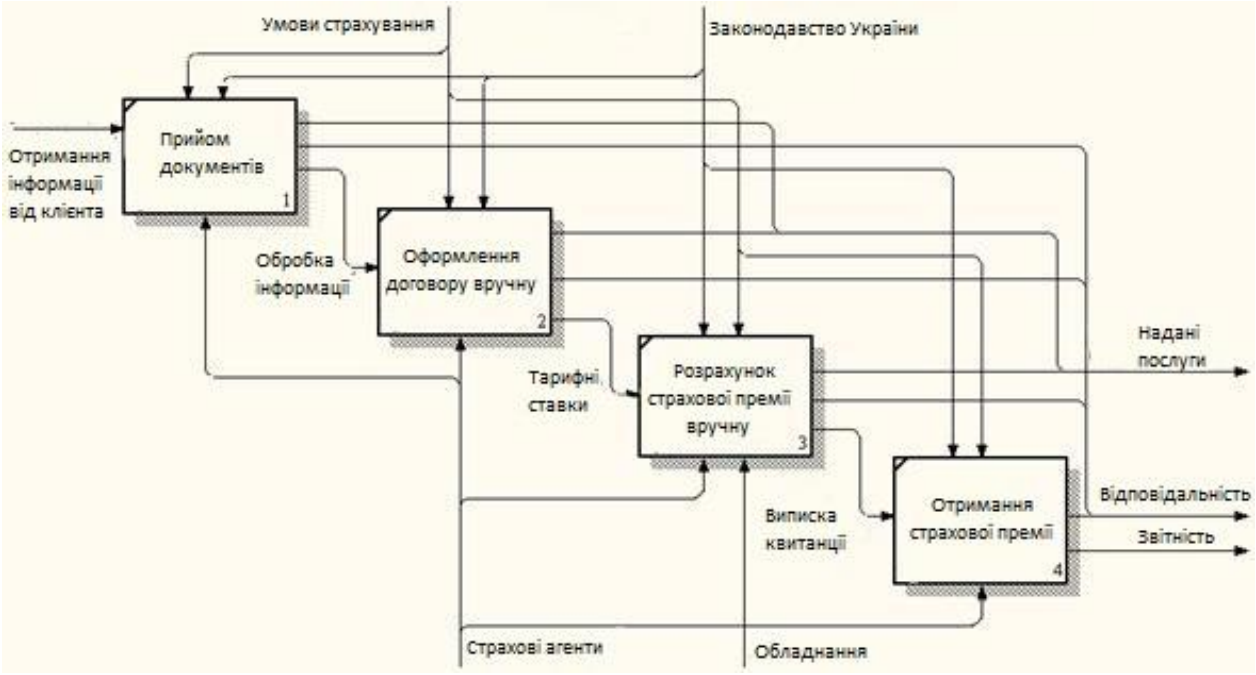

Рис. 3.5 Декомпозиція бізнес процесу заключення договору AS-IS.

При видачі страхового поліса страхувальнику робиться його копія, яка рухається всередині страхової компанії (рис. 3.6).

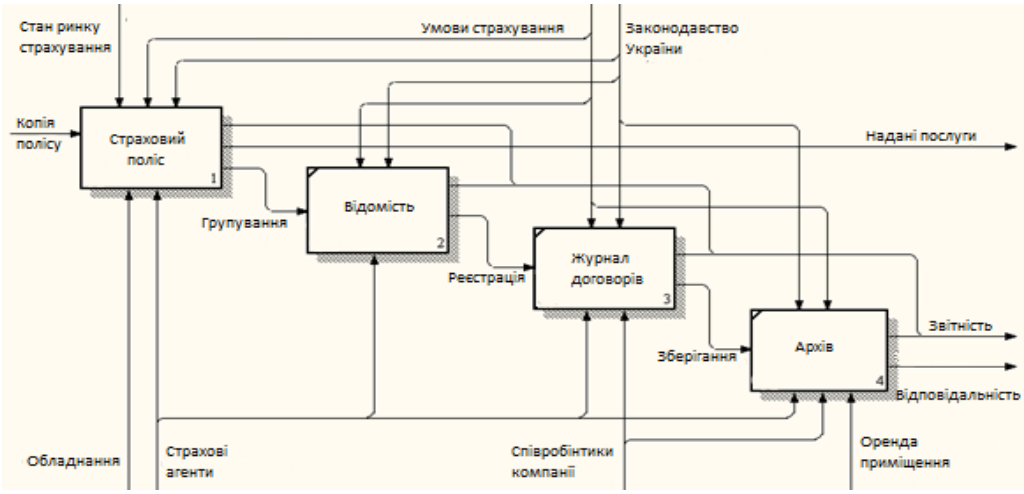

Рис. 3.6 Декомпозиція процесу руху страхового полісу в середині компанії.

Укладені страхові договори групуються у відомості та реєструються у журналі договорів, та був зберігаються у архіві компанії.

Страхувальник може внести зміни до укладеного раніше страхового договору, наприклад, переоформити його, додавши ще одного водія до списку осіб, допущених до керування транспортним засобом або навпаки зробити без обмеження осіб, допущених до керування.

А також поліс можна відновити (у разі втрати), переоформити, розірвати (якщо транспортний засіб збираються продати) або пролонгувати, тобто продовжити період використання транспортного засобу.

Діаграма бізнес-процесу можливих дій зі страховим полісом зображена на малюнку 3.7.

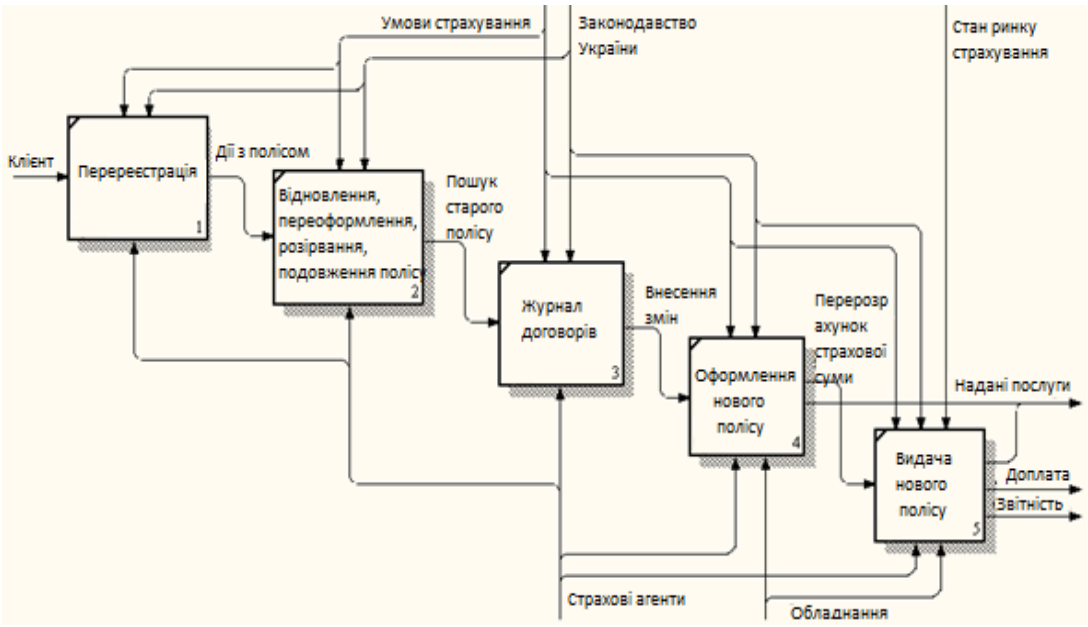

Рис 3.7 Декомпозиція бізнес процесу можливих дій зі страховим полісом AS-IS.

Декомпозиція бізнес-процесу укладання договорів страхування складається як з елементів, що містяться в функціональній моделі існуючих бізнес-процесів AS-IS (Рис. 3.5), так і нового елемента моделі TO-BE (Рис. 3.8).

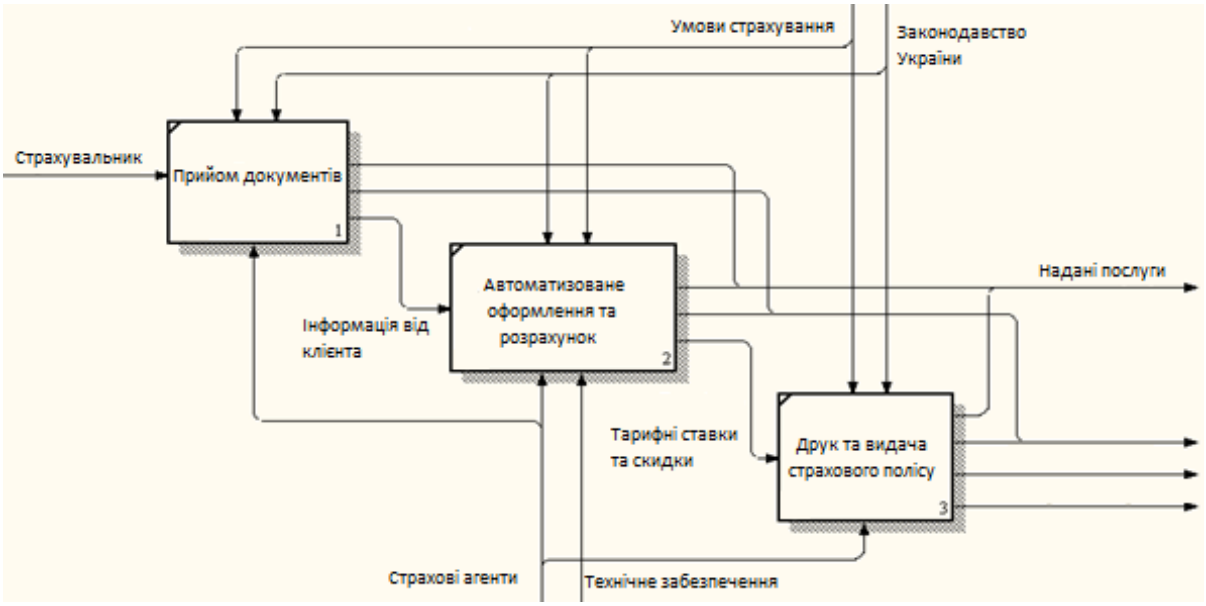

Рис. 3.8 Модель TO-BE декомпозиція бізнес процесу оформленння страхового полісу.

Модель ТО - ВЕ декомпозиції бізнес-процесу оформлення поліса складається з наступних бізнес-процесів:

- Прийом документів;
- Автоматизоване оформлення поліса та розрахунок страхової премії;
- Друк та видача страхового полісу.

Декомпозиція бізнес-процесу руху страхового поліса всередині страхової компанії також складається з елементів існуючого бізнес-процесу AS-IS (Рис. 3.6), так і нового елемента моделі TO-BE (Рис. 3.10).

Модель ТО – ВЕ складається з головного бізнес-процесу: створення інформаційної Клієнтської бази даних.

І декомпозиція бізнес процесу можливих дій зі страховим полісом складається з елементів, що містяться у функціональній моделі існуючих бізнес процесів AS-IS (Рис. 3.7) та нового елемента моделі TO-BE (Рис. 3.8).

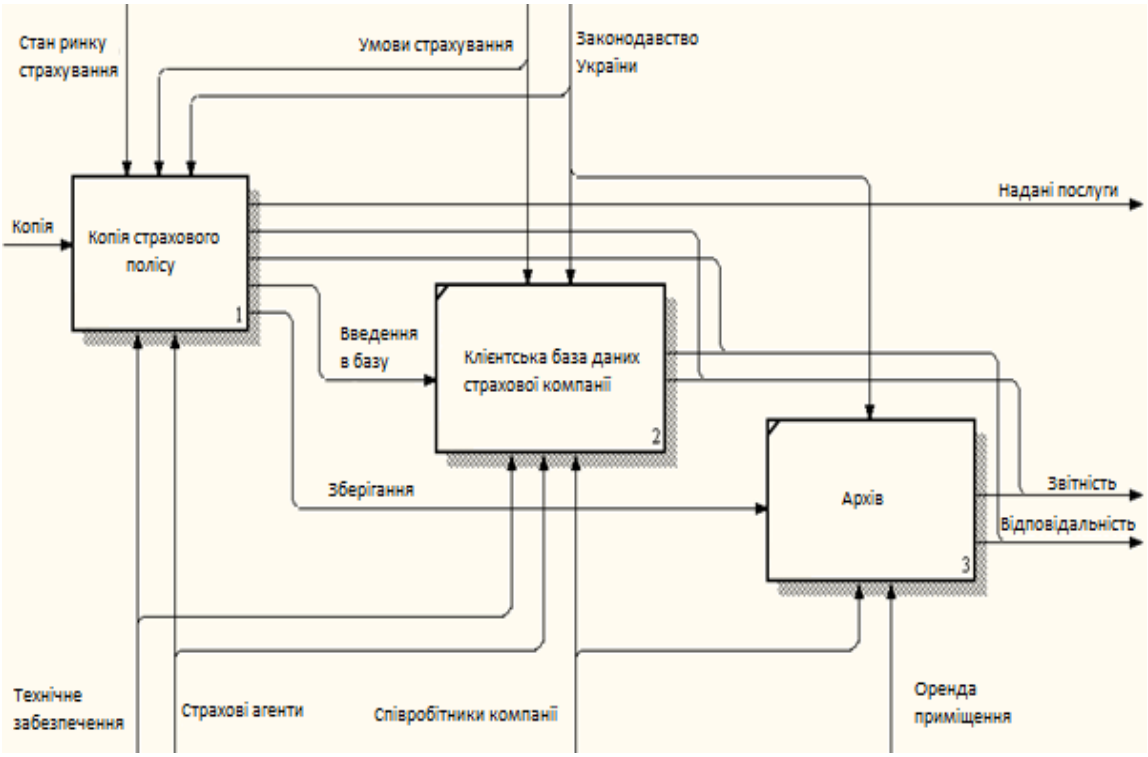

Рис. 3.9 Модель TO-BE декомпозиція бізнес процесу руху страхового полісу всередині страхової компанії.

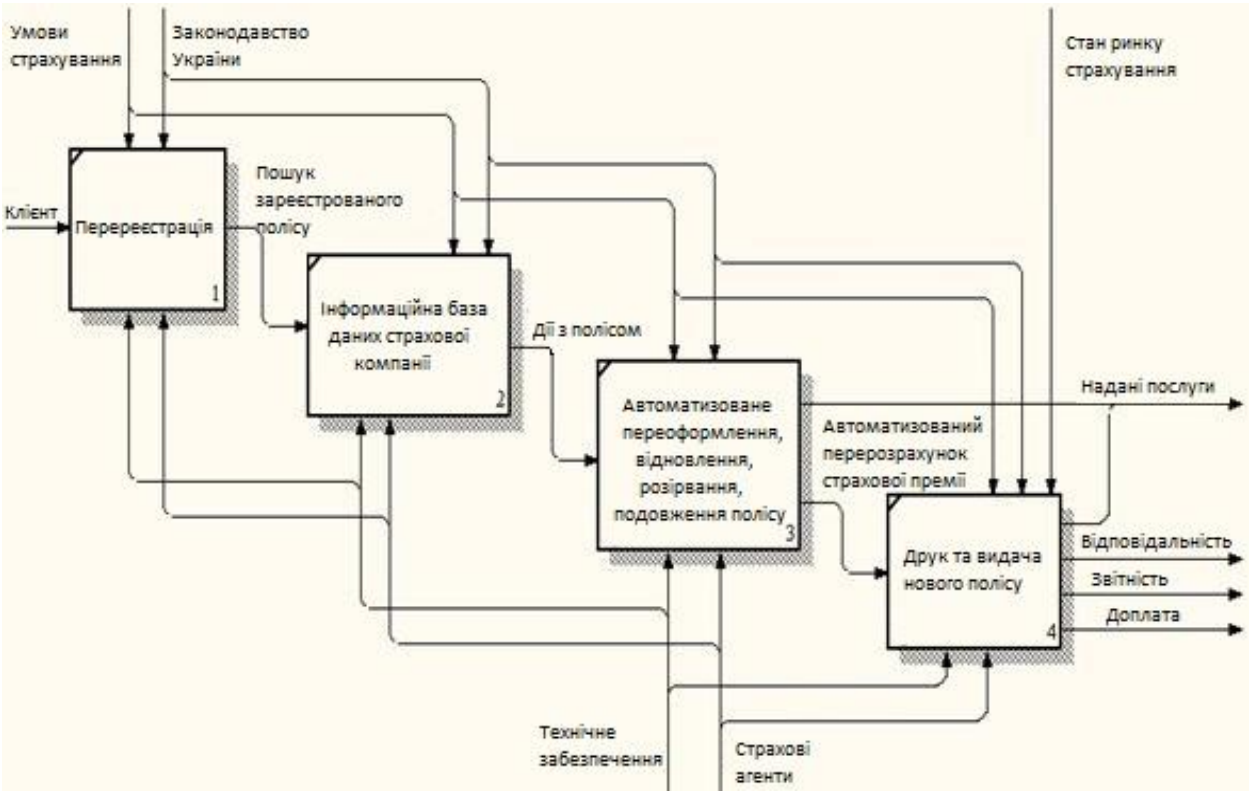

Рис. 3.10 Модель TO-BE бізнес процесу можливих дій зі страховим полісом

У Моделі ТО – ВЕ головним є «Інформаційна база даних» та «Автоматизоване переоформлення та перерахунок страхової премії», а також друк документа.

Основною перевагою моделі ТО-ВЕ є розширені можливості отримання статистичних і аналітичних даних. За рахунок впровадження ІС підвищиться продуктивність роботи додатків користувача, які дозволять оперативно взаємодіяти з клієнтами і вийти на якісно новий рівень їх обслуговування.

Таким чином, впровадження системи автоматизації обробки страхових документів передбачає комплекс організаційно-технічних заходів, які вирішують більшість перерахованих вище проблем.

Головною складовою інформаційної системи є створення єдиної інформаційної клієнтської бази, відомості про кожного клієнта та укладений з ним договір надійно зберігатимуться в центральній базі даних компанії.

Зрештою, при впровадженні інформаційної системи підвищиться оперативність управління ресурсами організації, виявляться її резерви та перспективи зростання для зміцнення позицій на ринку страхування. Інформаційна система страхової компанії, що розробляється, повинна усунути всі недоліки в роботі шляхом зниження витрат і збільшення обсягу страхування.

3.2 Розробка та реалізація методу захисту персональних даних клієнта

Згідно завдання дипломної роботи потрібно захистити дані клієнтів страхової компанії.

В результаті чого було прийнято рішення розробити такий метод перетворення даних, щоб за ними було складно відновити персональну інформацію та обґрунтувати коректність його роботи.

Метод було розроблено на високорівневій мові програмування Python з використанням середовища розробки NumPy. Причиною вибору даного програмного середовища стала зручна можливість роботи з багатовимірними масивами і матрицями, а також з розширеними можливостями роботи з високорівневими математичними функціями та моделями.

Реалізація та пояснення до алгоритму представлені нижче:

Алгоритм, має вісім основних пунктів.

1. *Запис у змінні ознак та цільової ознаки;*

features = data.drop('Страхові виплати', axis=1).values

target = data['Страхові виплати'].values

2. *Генерація випадкової матриці та перевірка її оборотності;*

Позначення:

- X - матриця ознак (нульовий стовпець складається з одиниць);
- y - вектор цільової ознаки;
- P - матриця, на яку множаться ознаки;
- ω - вектор ваги лінійної регресії (нульовий елемент дорівнює зрушенню);
- MSE – середня квадратична помилка;

Передбачення:

$$a = X\omega$$

Завдання на навчання:

$$\omega = \text{argmin}(\omega)\text{MSE}(X\omega, y)$$

Формула навчання:

$$\omega = (X^T X)^{-1} X^t y$$

Обгрнтування:

Замінимо вихідну матрицю X на якусь оборотну матрицю P:

$$N = XP$$

Розрахуємо вагу для нової матриці ωN:

$$\omega_n = (N^t N)^{-1} N^T y$$

Підставимо XP замість N:

$$\omega_n = ((XP^t)XP))^{-1}(XP)^T y$$

Почнемо розкривати дужки:

$$\omega_n = (P^T X^T (XP))^{-1} P^T X^T y$$

$$\omega_n = (X^T (XP))^{-1} P^T X^T y \text{ з цього слідує =>}$$

$$X^T (XP))^{-1} (P^{-1}) X^T y \text{ з цього слідує =>}$$

$$X^T (XP))^{-1} (P^{-1} P)^T X^T y$$

Матриця P обернена, а значить $(P)^{-1}P = \mathrm{E}$, де E – одична матриця, а також $\mathrm{E} = \mathrm{E}^T$:

$$\omega_n = (X^T(XP))^{-1}E^T X^T y \text{ з цього слідує =>}$$

$$((X^T X)P)^{-1}X^T y \text{ з цього слідує =>}$$

$$P^{-1}(X^T X)^{-1}X^T y$$

Відомо, що $\omega = (X^T X)^{-1}X^T y$, підставимо це в формулу ω_n:

$\omega_n = P^{-1}\omega$

Тепер розрахуємо передбачення для a_n для матриці N:

$a_n = N\omega_n = XPP^{-1}\omega$

Піднесення до степеня PP^{-1} дає одичну матрицю E:

$a_n = XE\omega = X\omega = a$

Цим самим ми довели, що передбачення a для матриці X рівнозначні передбаченням a_n для матриці (XP).

Програмна реалізація даного елементу:

```
matrix = np.random.normal(size = (4,4))
matrix array([
        [0.47084537, 0.80046089, -0.78646583, -0.69635017],
        [1.40685454, -1.66381486, 0.36380446, -0.06902221],
        [0.20149489, -0.65435128, -1.5307868, 1.39316897],
        [-0.17081503, 1.0498639, 0.22805616, -1.66327051]])
```

Перевіримо цю матрицю на обернення:

```
matrix = np.linalg.inv(matrix)
matrixarray([
        [1.45246724, 0.18756001, -0.90652865, -1.37519374],
        [1.25989914, -0.44415145, -0.94683918, -1.3021223],
        [0.27494229, -0.06642014, -0.94495611, -0.90385488],
        [ 0.68378635, -0.30871958, -0.6341161, -1.40583092]])
```

3. *Навчання моделі на вихідних ознаках;*

```
model = LinearRegression()
model.fit(features, target)
```

4. *Отримання метрики R2 на навченій моделі;*

   predictions = model.predict(features)

5. *Розмноження зворотної матриці на матрицю ознак;*

   features_new = features @matrix

6. *Навчання моделі на перетворених даних;*

   features_new = features @matrix

7. *Отримання мерики R2 на перетворених даних;*

   predictions_ = model.predict(features_new)

8. *Порівняння метрик.*

   print('R2 лінійної регресії:')

   print('вихідні ознаки --------',r2_score(target, predictions))

   print('перетворені ознаки -',r2_score(target, predictions_))

В даному проекті ставилося завдання захисту даних з допомогою перетворення даних. Було обрано метод перемноження ознак і випадкової зворотної матриці. Наведено теоретичне обґрунтування того, що таке перемноження не спотворить передбачень навченої таких даних моделі, в порівнянні з передбаченнями моделі, навченої на вихідних даних.

Здійснено навчання моделей на вихідних та перетворених даних та порівняно метрики R2 цих моделей. Метрики виявилися однаковими, що говорить про те, що нам удалося знайти спосіб шифрування даних без втрати якості роботи моделі. Задача виконана.

3.3 Опис розробленого програмного продукту

В ході написання кваліфікаційної роботи, було проаналізовано різноманітні варіанти розробки програмного засобу для забезпечення безпеки даних клієнтів страхової компанії в банківській сфері було прийняте рішення розробити Web-ресурс, для зручної взаємодії між банківською системою та фірмами, які займаються різнотипними видами страхування.

Оскільки основою будь-якого сайту є текстові документи, що містять керуючі символи, які визначають структуру та зовнішній вигляд сайту, вхідними даними для

вирішення поставленого завдання web-сайту буде текстова та графічна інформація. Текстова інформація представлена документами, відповідно графічна – ілюстраціями. Графічна інформація складається з фотографій та графічних файлів.

Нижче представлена інтерфейсна частина розробленого Web-ресурсу:

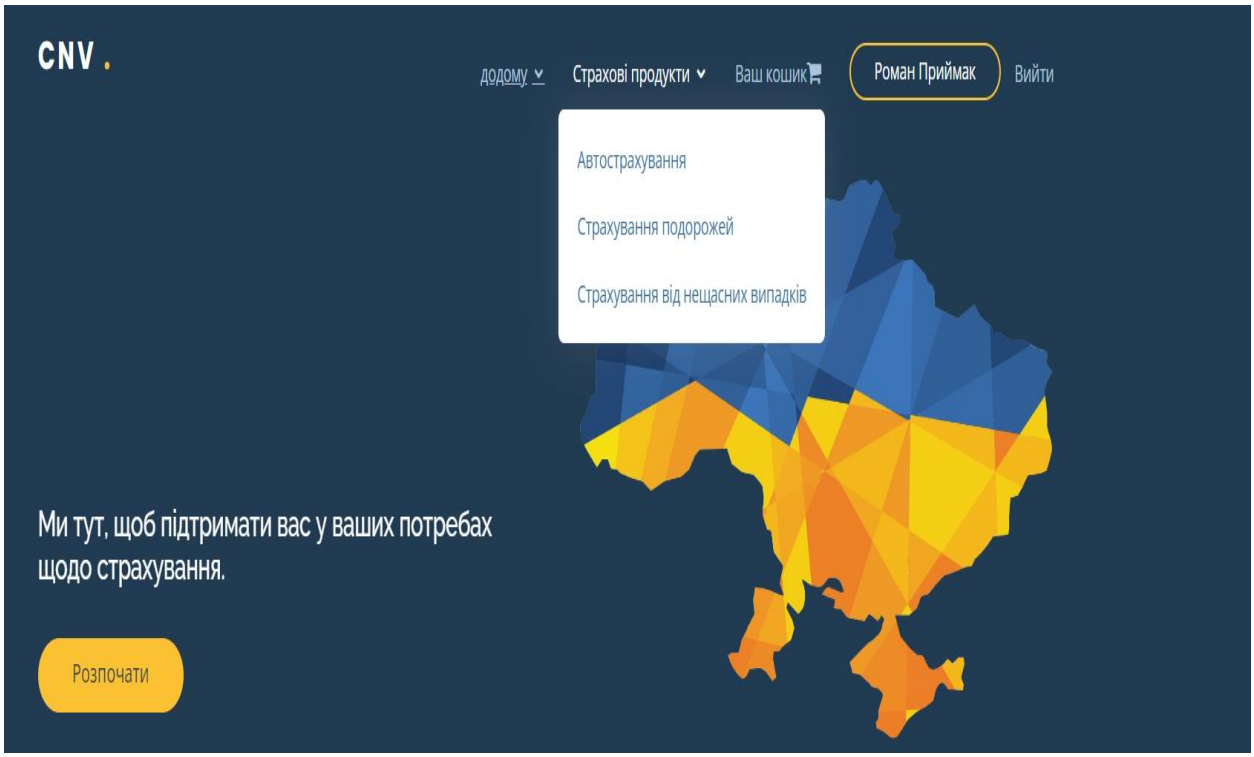

Рис. 3.11 Стартова сторінка Web-ресурсу

Стартова сторінка являє собою лице Web-ресурсу, а отже має виглядати так, щоб зацікавити користувача скористуватись даним сервіс.

Функціонал стартової сторінки бути інтуїтивно зрозумілим для користувача, тому він має декілька напрямків, по перше ви можете бачити, що є можливість авторизації на ресурсі (в подальшому планується розробити особистий кабінет). Також є варіативність вибору користувач може перейти конкретно на сторінки, котрі вказують на типи страхування, або натиснути кнопку “розпочати” та ознайомитися з інформацію на головній сторінці. Кнопка “розпочати” перенаправляє нас на ознайомлення та описом доступний на цей час типів

страхування (зараз доступне страхування подорожей, автострахування, та страхування здоров’я від нещасних випадків, що ви можете побачити на рис. 3.11).

Програмна реалізація основного елементу в розробленій сторінці представлена нижче в виді програмного коду на JavaScript, даний блок коду відповідає за відображення меню вибору послуг, та елементами які знаходяться на головній сторінці.

```
<main id="main">
    <!-- ======= Розділ клієнтів ======= -->
    <section id="clients" class="clients section-bg">
      <div class="container">
        <div class="row no-gutters clients-wrap clearfix wow fadeInUp">
          <div class="col-lg-2 col-md-4 col-6">
            <div class="client-logo">
              <img src="assets/img/clients/client-1.png" class="img-fluid" alt="" data-aos="flip-right">
            </div>
          </div>
          <div class="col-lg-2 col-md-4 col-6">
            <div class="client-logo">
              <img src="assets/img/clients/client-2.png" class="img-fluid" alt="" data-aos="flip-right"
data-aos-delay="100">
            </div>
          </div>
          <div class="col-lg-2 col-md-4 col-6">
            <div class="client-logo">
              <img src="assets/img/clients/client-3.png" class="img-fluid" alt="" data-aos="flip-right"
data-aos-delay="200">
            </div>
          </div>
          <div class="col-lg-2 col-md-4 col-6">
            <div class="client-logo">
              <img src="assets/img/clients/client-4.png" class="img-fluid" alt="" data-aos="flip-right"
data-aos-delay="300">
            </div>
          </div>

          <div class="col-lg-2 col-md-4 col-6">
            <div class="client-logo">
              <img src="assets/img/clients/client-5.png" class="img-fluid" alt="" data-aos="flip-right"
data-aos-delay="400">
            </div>
          </div>

          <div class="col-lg-2 col-md-4 col-6">
            <div class="client-logo">
              <img src="assets/img/clients/client-6.png" class="img-fluid" alt="" data-aos="flip-right"
data-aos-delay="500">
            </div>
          </div>
```

```
    </div>
  </div>
</section><!-- Розділ кінцевих клієнтів -->
```

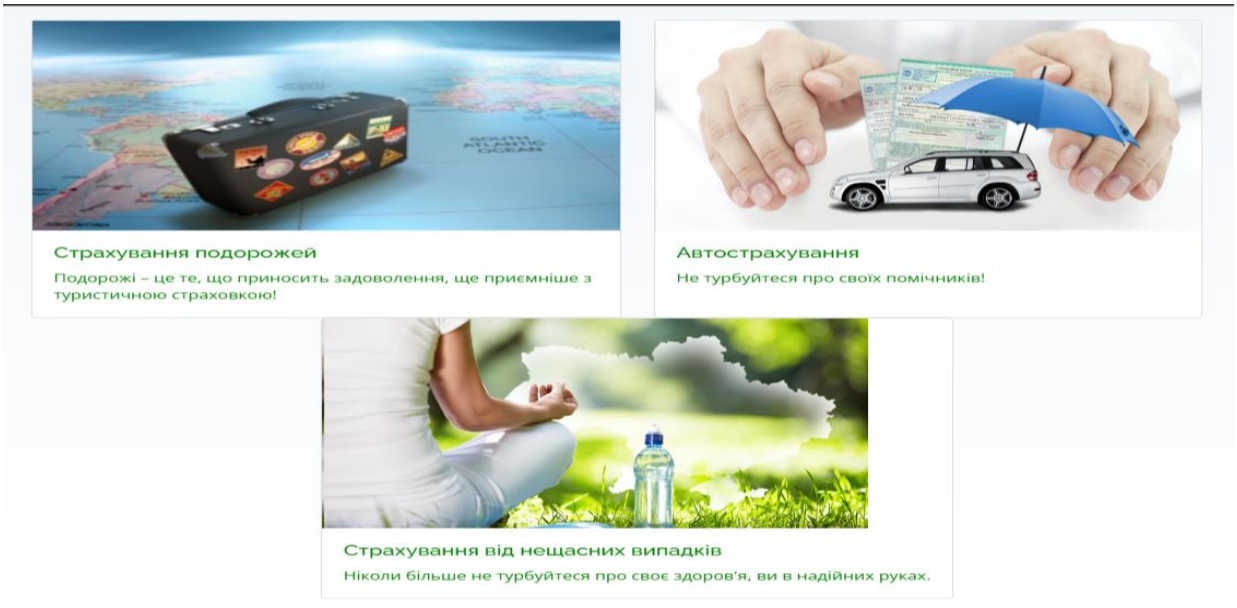

Рис. 3.11 Меню вибору типів страхування

Даний елемент програмного коду представляє собою відображення типів страхування та можливості з швидким ознайомленням клієнтом з доступними послугами які актуальні на даний момент, після ознайомлення дає можливість перейти в одне із доступних меню вибору страхування (зображених на рис 3.12-3.14).

```
<!-- ======= About Section ======= -->
<section id="about" class="about section-bg">
<div class="container">
<div class="row">
<div class="image col-xl-5 d-flex align-items-stretch justify-content-center justify-content-lg-start"></div>
<div class="col-xl-7 pl-0 pl-lg-5 pr-lg-1 d-flex align-items-stretch">
<div class="content d-flex flex-column justify-content-center">
<h3 data-aos="fade-in" data-aos-delay="100">A one stop portal to find your ideal insurance provider</h3>
<p data-aos="fade-in">
Having trouble finding the right insurance provider for you? Do banks offer you limited options? Want to find the best and cheapest option for you? SNV is here to save your day!
</p>
</div><!-- End .content-->
```

</section><!-- End About Section -->

Меню вибору типів страхування дає вам можливість ознайомитися з актуальними варіантами типів страхування та перейти кліком після вибору на потрібний для вас.

Розглянемо більш детально актуальні та доступні варіанти страхування: Вкладка страхування представляє собою. простий для користувача елемент інтерфейсу, задача якого швидко та інформативно ознайомити користувача з пропозиціями від різних страхових компаній та агентів.

Користувач може переглядати основну інформацію та при повторному натисканні клавіш на вибрану ним пропозицію, він може більш детально ознайомитися з пунктами, які входять в страховий поліс, при умові якщо користувача все влаштовує він може додати замовлення в корзину, та перейти до оплати. Якщо користувача не влаштовує вартість або умови страхового полісу він може далі ознайомлюватися з доступними пропозиціями.

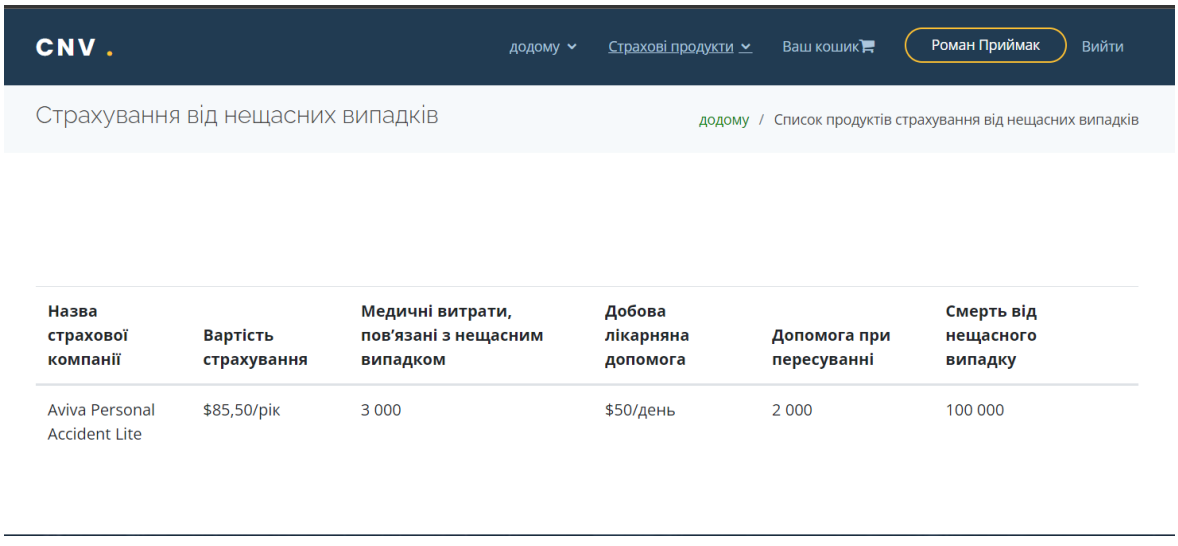

Рис. 3.12 Меню страхування від нещасних випадків

Програмна реалізація даного елементу виглядає наступним чином, ключовим елементом цієї сторінки є відображення таблиці з рядом параметрів вибраного типу страхування:

```
<main id="main">
    <section class="breadcrumbs">
      <div class="container">
        <div class="d-flex justify-content-between align-items-center">
          <h2>Страхування від нещасних випадків</h2>
          <ol>
            <li><a href="index.html">Домашня сторінка</a></li>
            <li>Список продуктів страхування від нещасних випадків</li>
          </ol>
          <!-- <input type="text" placeholder="Пошук продукту.."> -->
        </div>
      </div>
    </section><!-- End Breadcrumbs Section -->
<!-- додати цикл for для частини таблиці -->
    <section class="inner-page">
      <div class="container">
     <div class="col-md-12 text-right" >
        </div>
        <br><br>
        <table class="table table-hover">
          <head>
            <tr>
              <th scope="col">Назва страхової компанії</th>
              <th scope="col">Вартість страхування</th>
              <th scope="col">Медичні витрати, пов'язані з нещасним випадком</th>
              <th scope="col">Щоденна лікарняна допомога</th>
              <th scope="col">Допомога при пересуванні</th>
              <th scope="col">Смерть внаслідок нещасного випадку</th>
              <th scope="col"></th>
            </tr>
          </thead>
          <tbody id="tbody">
         <tr>
              <td>Aviva Personal Accident Lite</td>
              <td>$85,50/рік</td>
              <td>3000</td>
              <td>50 доларів США на день</td>
              <td>2000</td>
              <td>100 000</td>
            </tr>
          </tbody>
        </table>
      </div>
    </section>
```

На даному рисунку (рис.3.12) зображено актуальні та доступні пропозиції з області страхування від нещасних випадків. Де вказується назва страхової компанії, переліг послуг та ціни за які вони їх надають.

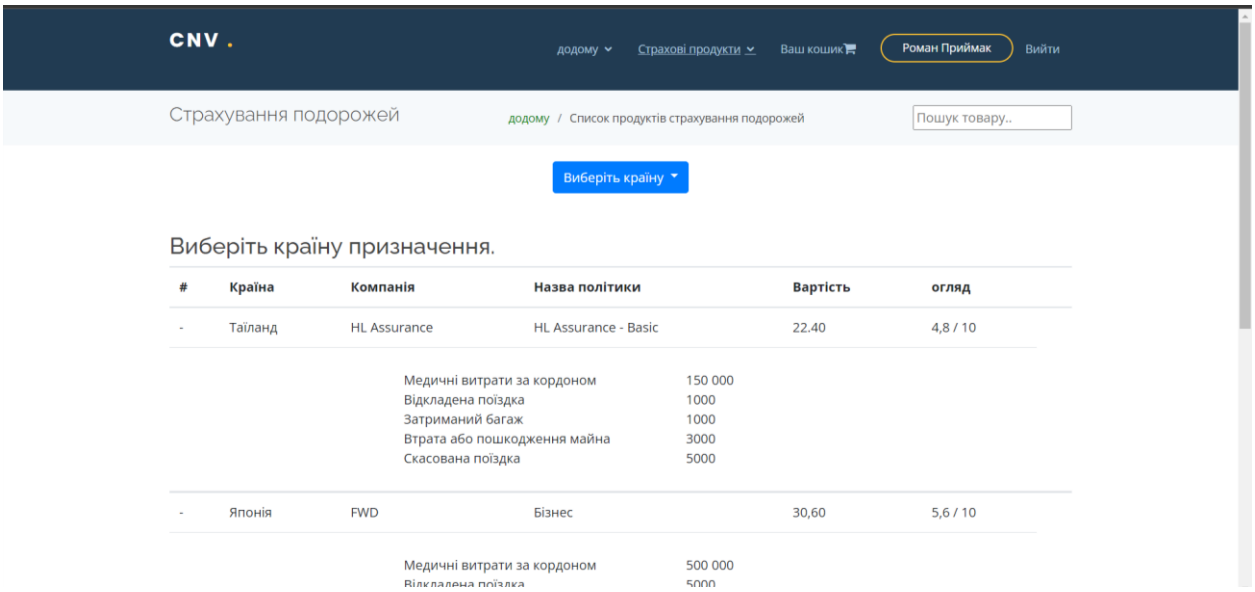

Рис. 3.13 Меню страхування подорожей

Меню страхування подорожей, на даний момент включає в себе декілька доступних пропозицій, і має більш детальний опис підпунктів страхових елементів, які входять в умову поліса при його оформленні.

Програмна реалізація даного елементу виглядає наступним чином:

```
<table class="table table-hover" id="table" style="visibility: visible;">
            <head>
              <tr>
                <th scope="col">#</th>
                <th scope="col">Країна</th>
                <th scope="col">Компанія</th>
                <th scope="col">Назва політики</th>
                <th scope="col">Вартість</th>
                <th scope="col">Огляд</th>
                <th scope="col"></th>
              </tr>
            </thead>
          <tbody id="tbody">
              <tr class="accordion-toggle collapsed" id="accordion1" data-toggle="collapse" data-parent="#accordion1" href="#collapse1">
                <td class="expand-button"></td>
                <td>Таїланд</td>
                <td>Гарантія HL</td>
                <td>HL Assurance - Basic</td>
                <td>22.40</td>
                <td>4,8 / 10</td>
              </tr>
```

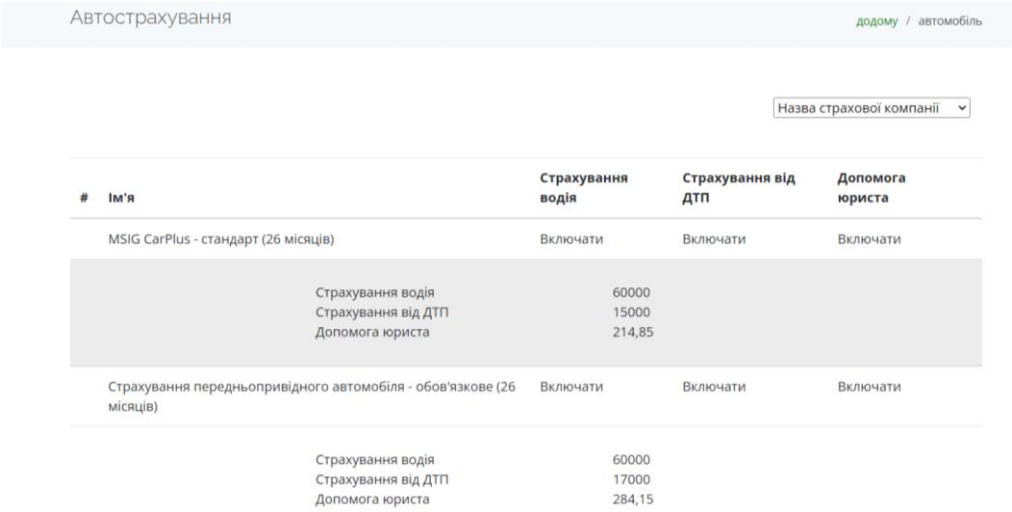

Рис. 3.14 Меню автострахування

Меню автострахування праює про принципу попереднього, але є нюанс, що користувачу необіхдно вибирати поліс страхування згідно технічних характеристик та типу його автомобіля.

Програмна реалізація даного елементу виглядає наступним чином:

```
Selection class="breadcrumbs">
        <div class="container">
          <div class="d-flex justify-content-between align-items-center">
            <h2>Страхування автомобіля</h2>
            <ol>
              <li><a href="index.html">Домашня сторінка</a></li>
              <li>Автомобіль
          <!-- <input type="text" placeholder="Пошук продукту.."> -->
          </div>
        </div>
      </section><!-- End Breadcrumbs Section -->
<!-- додати цикл for для частини таблиці -->
      <section class="inner-page">
        <div class="container">
          <div class="col-md-12 text-right" >
            <select name = "filter">
              <option value = "lowHigh"> Назва страхової компанії </option>
              <option value = "lowHigh"> Ціна: від низького до високого </option>
```

```
            <option value = "lowHigh"> Ціна: від високої до низької </option>
          </select>
        </div>
        <br><br>
<!-- <table class="table table-hover">
          <head>
            <tr>
              <th scope="col">Ім'я</th>
              <th scope="col">Страхування водія</th>
              <th scope="col">Страхування від нещасних випадків</th>
              <th scope="col">Допомога юриста</th>
              <th scope="col"></th>
            </tr>
    </thead>
          <tbody id="tbody">
            <tr>
              <td>1</td>
              <td>2</td>
              <td>3</td>
              <td>4</td>
            </tr>
```

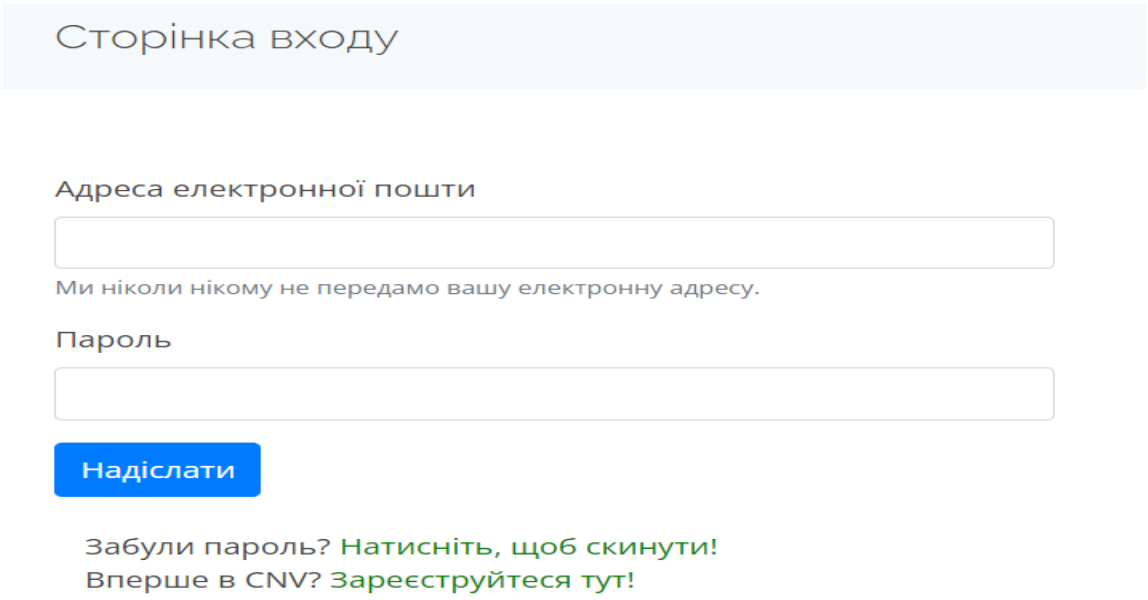

Рис. 3.15 Інтерфейсне вікно сторінки входу

Перед початком оплати користувачу необхідно авторизуватись на Web-ресурсі, щоб ідентифікувати свою особу та задля можливості страховим компаніям ідентифікувати дані клієнта через BankID.

На сторінці авторизації зображено інтерфейсне меню авторизації або реєстрації на Web-ресурсіпрограмна реалізація даної веб сторінки виглядає наступним чином:

```
<section class="inner-page">
        <div class="container">
        <form>
          <div class="form-group">
              <label for="exampleInputEmail1@gmail.com">Адреса електронної пошти</label>
              <input type="email" class="form-control" id="Email1@gmail.com" aria-describedby="emailHelp" style = "width:500px;"/>
              <small id="emailHelp" class="form-text text-muted">Ми ніколи нікому не повідомлятимемо вашу електронну адресу.</small>
          </div>
          <div class="form-group">
              <label for="exampleInputPassword1">Пароль</label>
              <input type="password" class="form-control" id="password1" style = "width:500px;">
          </div>
          <button type="submit" class="btn btn-primary">Надіслати</button>
          <br><br>

          <div class="container">
            <span class="psw">Забули пароль?<a href="reset_password.html"> Натисніть, щоб скинути!</a></span> <br>
              <span class = "signup" >Новий користувач CNV? <a href = "signup.html">Зареєструйтеся тут!</a> </span>
          </div>
        </form>
          </div>
        </section>
```

На сьогодні реалізована можливість працювати з трьома платіжними методами.

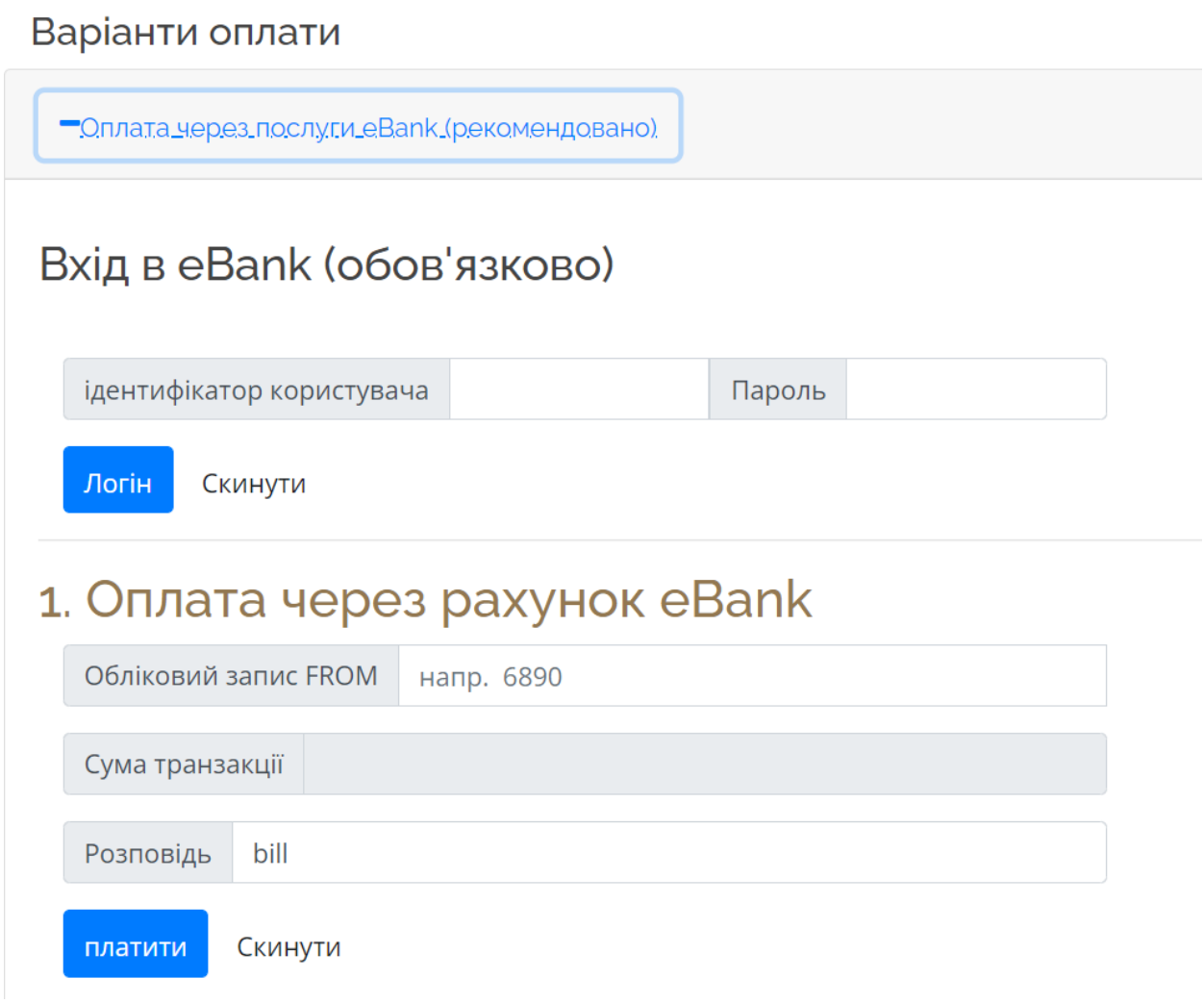

Рис. 3.16 Перший з трьох методів оплати. Оплата з банківського рахунку

Перший з платіжних методів це оплата безпосередньо з банківського рахунку користувача, з будь-якого банку, якщо це дозволяє законодавство країни де знаходиться клієнт на даний момент без посередньо.

Програмна реалізація даного елементу виглядає наступним чином:

```
<!-- API оплати рахунків-->
                        <h2 style="color:#937851">1. Оплата через рахунок eBank</h2>
                        <div class="col-md-6">
                          <form class="form-horizontal well" style="padding-bottom: 0px;">
                            <div class="input-group mb-3">
                              <div class="input-group-prepend">
                              <span class="input-group-text">Обліковий запис FROM</span>
                              </div>
                              <input id="accountFrom" type="text" class="form-control" placeholder="
наприклад, 6890">
                              <input id="accountTo" type="text" value= "6699" class="form-control"
hidden>
                            </div>
```

```
                        <div class="input-group mb-3">
                          <div class="input-group-prepend">
                          <span class="input-group-text">Сума трансакції</span>
                          </div>
                          <input id="transactionAmount" type="text" class="form-control">
                        </div>
                          <input id="transactionReferenceNumber" value="100" type="text"
class="form-control" placeholder="10" hidden>
                        <div class="input-group mb-3">
                          <div class="input-group-prepend">
                          <span class="input-group-text">Розповідь</span>
                          </div>
                          <input id="narrative" type="text" value="bill" class="form-control"
placeholder="10">
                        </div>
                        <div style="color: red;" id="помилка"></div>
                        <div class="form-group">
                          <button id="Send" type="button" class="btn btn-primary
Send">Оплатити</button>
                          <button type="reset" class="btn btn-default">Скинути</button>
                        </div>
                      </form>
                    </div>
```

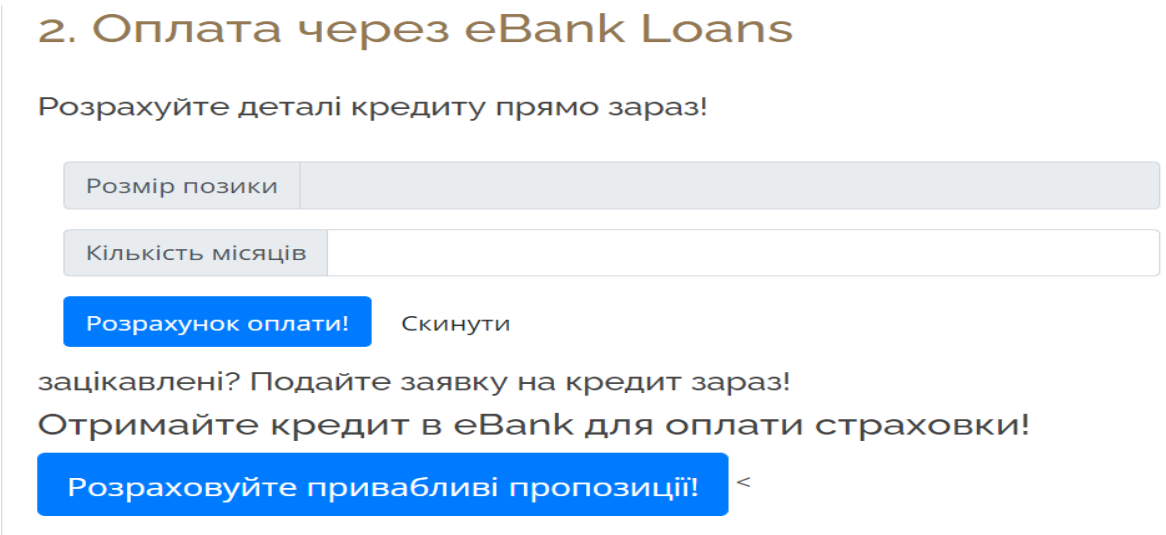

Рис. 3.17 Другий з трьох методів оплати. Отримання страхового кредиту.

Наступний метод це отримання страхового кредиту, це дає можливість клієнту отримати кредит на будь-який тип страхування, за умови, що в нього немає проблем с кредитною історією. Даний метод запущений в тестовому режимі, через це в деякі періоди можуть виникнути технічні несправності, тому клієнтам рекомендується використовувати платіжні методи один та три.

Програмна реалізація даного елементу виглядає наступним чином:

```
!-- API позики -->
                        <h2 style="color:#937851">2. Оплата через eBank Loans</h2>
                        <br>
                        <h5> Розрахуйте деталі кредиту зараз!</h5>
                        <br/>
                    <div class="col-md-6">
                      <form>
                        <input id="LoanproductID" type="text" class="form-control" value="201" hidden/>
                        <div class="input-group mb-3">
                          <div class="input-group-prepend">
                          <span class="input-group-text">Сума позики</span>
                          </div>
                          <input id="requestedAmount" type="text" class="form-control">
                        </div>
                        <div class="input-group mb-3">
                          <div class="input-group-prepend">
                          <span class="input-group-text">Кількість місяців</span>
                          </div>
                          <input id="LoannumberOfMonths" type="text" class="form-control">
                        </div>
                        <div class="form-group">
                          <button id="RequestLoan" type="button" class="btn btn-primary">Розрахувати платіж!</button>
                          <button type="Lreset" class="btn btn-default">Скинути</button>
                        </div>
                        <div style="color: red;" id="LoanRequestError"></div>
                      </form>
                      </div>
```

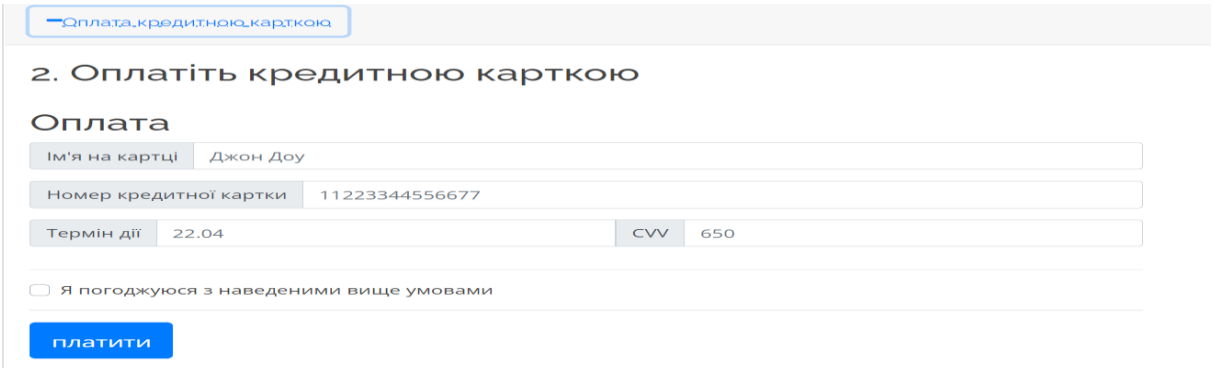

Рис. 3.18 Третій з методів оплати. Оплата кредитною картою

Третій метод являє собою оплату кредитною картою, що на мою думку є більш звичним та зручним для громадян України. Він реалізований стандартним для цього методу оплати способом:

- Ввід даних відправника платіжна (ФІО);

- Номер кредитної або дебетової карти;
- Термін дії;
- CVV або CVC.

Система не зберігає дані від карт користувачів.

Програмна реалізація даного елементу виглядає наступним чином:

```
<div class="card">
                    <div class="card-header" id="headingTwo">
                        <h2 class="mb-0">
                            <button type="button" class="btn btn-link collapsed" data-toggle="collapse" data-target="#collapseTwo"><i class="fa fa-plus"></i> Оплата кредитною карткою </button>
                        </h2>
                    </div>
                    <div id="collapseTwo" class="collapse show" aria-labelledby="headingTwo" data-parent="#accordionExample">
                        <div class="card-body">
                          <div class="row">
                            <div class="col-lg-8 col-md-8 col-sm-7 col-xs-12">
                              <h2>2. Оплатіть кредитною карткою</h2>
                              <br>
                            <div class="input-group mb-3">
                              <h2>Оплата</h2>
                                <div class="input-group mb-3">
                                <div class="input-group-prepend">
                                <span class="input-group-text" id="nameoncard">Ім'я на картці</span>
                                </div>
                                <input type="text" class="form-control" placeholder="John Doe" aria-label="nameoncard" aria-describedby="basic-addon1">
                            </div>
                            <div class="input-group mb-3">
                              <div class="input-group-prepend">
                              <span class="input-group-text" id="nameoncard">Номер кредитної картки</span>
                              </div>
                              <input type="text" class="form-control" placeholder="11223344556677" aria-label="номер кредитної картки" aria-describedby="basic-addon1">
                            </div>
                            <div class="input-group mb-3">
                              <div class="input-group-prepend">
                              <span class="input-group-text" id="expiration">Термін дії</span>
                              </div>
                              <input type="text" class="form-control" placeholder="04/22" aria-label="expiration" aria-describedby="basic-addon1">
                              <div class="input-group-prepend">
                              <span class="input-group-text" id="cvv">CVV</span>
                              </div>
                              <input type="text" class="form-control" placeholder="650" aria-label="cvv" aria-describedby="basic-addon1">
                            </div>
                          </div>   <hr>
```

3.4 Засоби які використовувалися для розробки програмного засобу

Web-сайт складається із пов'язаних між собою Web-сторінок. Web-сторінка є текстовим файлом з розширенням *.htm, який містить текстову інформацію та спеціальні команди – HTML-коди, що визначають у якому вигляді ця інформація буде відображатися у вікні браузера. Вся графічна, аудіо- та відео-інформація безпосередньо в Web-сторінку не входить і є окремими файлами з розширеннями *.gif, *.jpg (png), *.mid, *.mp3,*.avi (mp4). HTML-код сторінки містить лише вказівки на такі файли.

Кожна сторінка Web-сайту також має свою Internet адресу, яка складається з адреси сайту та імені файлу, що відповідає даній сторінці. Таким чином, Web-сайт це інформаційний ресурс, що складається із пов'язаних між собою гіпертекстових документів (Web-сторінок), розміщений на Web-сервері та має індивідуальну адресу. Переглянути Web-сайт може будь-яка людина, має комп'ютер, підключений до Internet.

Середовище розробки Atom:

Такі редактори як Sublime та TextMate пропонують зручність, але лише обмежені можливості розширення. З іншого боку, Emacs та Vim пропонують дивовижну гнучкість, але вони не дуже доступні та можуть бути налаштовані лише за допомогою спеціальних мов сценаріїв.

Мета розробки атома — безкомпромісне поєднання можливостей та зручності використання: редактор, який сподобається учневі початкової школи у перший день навчання програмуванню, а також інструмент, який він не переросте, коли стане досвідченим програмістом.

На перший погляд, Atom – це сучасний текстовий редактор для робочого столу, на який ви звикли чекати.

- Ядро атома

Інтернет не позбавлений недоліків, але два десятиліття розвитку перетворили його на неймовірно пластичну та потужну платформу. Отже, коли було вирішено написати текстовий редактор, веб-технологія була очевидним вибором.

- Рідна мережа

Веб-браузери чудово підходять для перегляду веб-сторінок, але написання коду – це спеціальна діяльність, яка потребує спеціальних інструментів. Що ще важливіше, браузер суворо обмежує доступ до локальної системи з міркувань безпеки, і для нас текстовий редактор, який не міг писати файли або запускати локальні підпроцеси, не був потрібним.

Тому Atom не створювали як традиційний веб-додаток. Атом є спеціалізованим варіантом Chromium, розробленим як текстовий редактор, а чи не браузер. Шкірне вікно Atom – це, насправді, локально відтворена веб-сторінка.

Усі API, доступні за замовчуванням Node.js, також доступні для коду, який виконується в контексті JavaScript кожного вікна. Цей гібрид забезпечує унікальний досвід розробки за клієнта.

Оскільки все локально, вам не доведеться турбуватися про конвеєри ресурсів, конкатенацію сценаріїв та асинхронні визначення модулів. Якщо ви хочете завантажити будь-який код, просто вимагайте його у верхній частині файлу. Модульна система Node дозволяє легко розбити систему на безліч невеликих цілеспрямованих пакетів.

JavaScript, C++

Взаємодія з рідним кодом також дуже проста. Крім API Node Atom також надає API для своїх діалогів, додавання програм і пунктів контекстного меню, управління розмірами вікна і т.д.

- Веб-технології:

Ще одна велика перевага, яка приносить написання коду для Atom – це гарантія того, що він працює на новітній версії Chromium. Це означає, що ми можемо ігнорувати такі проблеми, як сумісність браузера та полізаповнення. Ми можемо використовувати всі блискучі функції Інтернет завтра, сьогодні.

Наприклад, макет нашої робочої області та панелей базується на flexbox. Це новий стандарт, який пережив багато змін відколи ми почали його використовувати, але все це не мало значення, поки він працював.

Оскільки вся індустрія просуває веб-технології вперед, ми впевнені, що будуємо Atom на благодатному грунті. Власні технології інтерфейсу користувача

приходять і йдуть, але Інтернет – це стандарт, який з кожним роком стає все більш потужним та повсюдним. Ми раді глибше вивчити його інструментарій.

Текстовий редактор із відкритим кодом

Ми розглядаємо Atom як ідеальне доповнення до основної місії GitHub – створення кращого програмного забезпечення шляхом спільної роботи. Atom – це довгострокова інвестиція, і GitHub продовжуватиме підтримувати його розвиток за допомогою спеціальної команди. Але ми також знаємо, що ми не можемо досягти нашого бачення Atom поодинці. Як Emacs і Vim продемонстрували за останні три десятиліття, якщо ви хочете побудувати процвітаючу, довготривалу спільноту навколо текстового редактора, вона має бути з відкритим кодом.

Мова програмування JavaScript:

JavaScript — це мова програмування. Багато з них пов’язані з тим, що JavaScript часто виконується безпосередньо в браузері клієнта, який зазвичай використовується у веб-розробці.

JavaScript може бути мовою сценаріїв на стороні клієнта, що означає, що текстовий файл ASCII обробляється браузером клієнта, а не на онлайн-сервері. Це може завантажити веб-сторінку без зв’язку з головним сервером за допомогою JavaScript. Наприклад, функція JavaScript може перевірити Інтернет-форму перед її надсиланням, щоб переконатися, що всі вказані поля заповнені. Код JavaScript може видати повідомлення про помилку до того, як будь-яка інформація дійсно буде передана на сервер.

Подібно до серверних мов сценаріїв, таких як PHP і ASP, код JavaScript часто вставляється будь-де в HTML-код веб-сторінки. Вихід на стороні сервера відображається в HTML, але код JavaScript залишається видимим у вихідному коді веб-сторінки. Файл може бути окремим файлом «.js», який можна відобразити у браузері.

JavaScript має деякі переваги та недоліки. JavaScript часто виконується безпосередньо в браузері клієнта. JavaScript також може мати ті ж переваги, що й серверні мови.

Переваги JavaScript:

- Незалежно від того, де ви розміщуєте JavaScript, він завжди виконується в клієнтському середовищі, щоб заощадити значну пропускну здатність і зробити процес виконання швидким;
- Найбільшою перевагою JavaScript є можливість підтримувати всі сучасні браузери та створювати еквівалентний результат;
- JavaScript використовується всюди в Інтернеті;
- JavaScript чудово поєднується з іншими мовами та може використовуватися у величезній кількості програм;
- Існує багато проектів з відкритим вихідним кодом, які надають корисну допомогу розробникам у додаванні JavaScript;
- Є багато доступних курсів у галузі JavaScript, завдяки яким ви швидко та просто розширите свої знання цієї мови програмування.

Недоліки JavaScript:

- Це може бути складно для розробки великих програм, хоча ви також будете використовувати накладення TypeScript.
- Основна проблема або недолік JavaScript полягає в тому, що код завжди видимий для всіх, хто може переглядати код JavaScript.
- Незалежно від того, яку частку інтерпретує швидкий JavaScript,
- JavaScript DOM (модель об’єктів документа) є повільним і ніколи не може бути швидким рендерингом у HTML.
- Якщо помилка виникає в JavaScript, він може припинити відтворення всього веб-сайту. Браузери надзвичайно терпимі до помилок JavaScript.
- Зазвичай JavaScript по-різному інтерпретується різними браузерами. Це дещо ускладнює читання та написання кросбраузерного коду
- Хоча деякі редактори HTML підтримують налагодження, вони не такі ефективні, як інші редактори, наприклад редактори C/C++. Тому розробнику важко виявити проблему.

Приклад використання мови JavaScript в контесті виконання завдання кваліфікаційної роботи:

```
//Розбиття таблиці
```

```
<tr class="show-table-padding">
        <td colspan="6">
          <div id="collapse1" class="collapse in p-3">
            <div class="row">
              <div class="col-3"></div>
              <div class="col-4">Driver insurance</div>
              <div class="col">60000</div>
            </div>
            <div class="row">
              <div class="col-3"></div>
              <div class="col-4">Car accident insurance</div>
              <div class="col">15000</div>
            </div>
            <div class="row">
              <div class="col-3"></div>
              <div class="col-4">Assistance of a lawyer</div>
              <div class="col">214.85</div>
            </div>
            <tbody id="tbody">
                <tr class="accordion-toggle collapsed" id="accordion1" data-toggle="collapse" data-parent="#accordion1" href="#collapse1">
                  <td class="expand-button"></td>
                  <td>FWD Car Insurance - Essential (26 months)</td>
                  <td>Include</td>
                  <td>Include</td>
                  <td>Include</td>
                </tr>
```

Мова тегів HTML:

HTML, або мова гіпертекстової розмітки, — це мова розмітки для Інтернету, яка визначає структуру веб-сторінок.

Це один із найпростіших будівельних блоків кожного веб-сайту, тому вкрай важливо навчитися цьому, якщо ви хочете зробити кар’єру у веб-розробці.

Щоб зрозуміти "HTML" від початку до кінця, давайте подивимось на кожне слово, що входить до складу абревіатури:

- Гіпертекст: текст (часто також із вбудованими зображеннями), організований для з’єднання пов’язаних елементів;
- Розмітка: посібник зі стилю для верстки всього, що буде надруковано у паперовому або електронному форматі;
- Мова : мова, яку комп’ютерна система розуміє та використовує для інтерпретації команд.

HTML визначає структуру веб-сторінок. Однієї цієї структури недостатньо, щоб зробити веб-сторінку гарною та інтерактивною. Таким чином, ви будете використовувати допоміжні технології, такі як CSS і JavaScript, щоб зробити свій HTML красивим і додати інтерактивності відповідно.

Приклад використання мови HTML в контесті виконання завдання кваліфікаційної роботи:

```
//створення заголовку
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <title>View Products</title>
  <meta content="" name="descriptison">
  <meta content="" name="keywords">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <!-- Favicons -->
  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

Мова стилю сторінок CSS:

CSS (абревіатура від Cascading Style Sheets, що в перекладі означає каскадні таблиці стилів) - це спеціальна мова (мова стилів), за допомогою якої описують вигляду документів (як і де відображати елементи веб-сторінки), написаних мовами розмітки даних. Найчастіше CSS використовується для документів, котрі розмічені мовою HTML, XHTML та XML.

Одна з головних переваг використання CSS - це можливість розділити зміст сторінки від її оформлення. Таке розділення дозволило покращити сприйняття та доступність змісту, забезпечити більшу гнучкість та контроль за відображенням змісту в різних умовах, зробити зміст більш структурованим та простим, прибрати повторення та ін. Власне це ж і була основна мета створення цієї технології.

Що дає використання CSS:

Відображати один і той же документ в різних стилях.

Декілька дизайнів сторінки для різних пристроїв. Наприклад, на екрані дизайн буде розрахований на велику ширину, під час друку меню не виводитиметься, а на смартфоні меню буде внизу, під вмістом.

Зменшення часу завантаження сторінок сайту за рахунок перенесення правил відображення в окремий CSS-файл. В цьому випадку браузер завантажує тільки структуру документа і дані, що зберігаються на сторінці, а стильові правила цих даних завантажуються браузером тільки один раз і кешуються.

Простота подальшої зміни дизайну. Не потрібно правити кожну сторінку, а лише змінити CSS-файл.

Додаткові можливості оформлення. Наприклад, за допомогою CSS-розмітки можна зробити так, щоб меню було завжди видно при скролінгу сторінки, або прибрати підкреслення у посилань.

Дозволяє створювати складну і пропрацьовану техніку дизайну.

Правила в CSS працють по каскаду (пріорітету, вазі). Це дозволяє отримати передбачуваний результат у випадку, коли до одного елемента, одночасно, застосовуються декілька стильових правил.

Приклад використання мови HTML в контесті виконання завдання кваліфікаційної роботи:

```
label {
    font-weight: 500;
}
.forgot-password,
.forgot-password a {
    text-align: right;
```

```
    font-size: 13px;
    padding-top: 10px;
    color: #7a7a7a;
    margin: 0;
}
.forgot-password a {
    color: #2554FF;
}
```

3.5 Висновки до розділу

В ході написання третього розділу кваліфікаційної роботи, було розроблено інформаційну модель діяльності страхової компанії з подальшим розбиттям її на рівні декомопзиції, та змістове пояснення до них.

Наступним пунктом стала розробка алгоритму захисту персональних данних клієнта, структора якого базується на лінійній алгебрі та матетичне доведення дієздатності алгоритму с подальшою реалізацією на високорівневій об’єктно-орієнтованій мові програмування Pyhton.

В розділі згідно завдання кваліфікаційної роботи, було розроблено Web-ресурс за допомогою мови програмування JavaScript, для можливості взаємодії між банками та страховими компаніями. Та ілюстративно зображено основний функціонал роботи ресурсу, з поясненням як він реалізовувався програмно.

Висновки

В ході написання кваліфікаційної роботи, було досліджено поняття інформаційної безпеки та різні ви плаваючі з цього аспекти, було розглянуто безпеку інформаційних систем та елементи її захисту.

Інформаційна безпека має вирішальне значення в організації. Усю інформацію, що зберігається в організації, слід зберігати в безпеці. Інформаційна безпека буде визначена як захист даних від будь-яких вірусних загроз. Інформаційна безпека важлива в організації, оскільки вона може захистити конфіденційну інформацію, забезпечує роботу організації, а також забезпечує безпечну роботу додатків, реалізованих у системі інформаційних технологій організації, а інформація є активом для організації.

Навіть незважаючи на те, що інформація є важливою для організації, є кілька проблем, пов'язаних із захистом інформації та керування нею. Одним із викликів, з якими стикається організація, є відсутність розуміння важливості інформаційної безпеки.

Коли співробітникам бракує знань з інформаційної безпеки щодо збереження їх інформації, організація легко піддається атакам хакерів або інших загроз, які намагаються викрасти або отримати конфіденційну інформацію організації.

В другому розділі кваліфікаційної роботи було розглянуто загрози інформаційним системам включаю людський фактор. Та розглянуто теоретично, можливість реалізації страхових систем в банківські.

Співпраця банків та страхових компаній є вигідною і для споживачів послуг останніх. Зазвичай, вигоди клієнтів проявляються в зручності при отриманні послуг, а також економії коштів та часу на їх оформлення. При цьому, недоліком банківського страхування може бути падіння довіри до банківської установи з боку тих клієнтів, які вважатимуть інтегровані продукти непотрібними чи нав'язливими.

Факт розголошення банком конфіденційних даних клієнтів, останніми також сприймається з недовірою. Успішність інтеграції в багатьох випадках залежить від здатності банка та страховика вчасно реагувати на загрози, які існують на фінансовому ринку і безпосереднім чином можуть вплинути на економічні інтереси

фінансових посередників. Хоча сьогодні банки і страхові компанії працюють в складних умовах, але банківське страхування в Україні має досить великий потенціал для розвитку. В ході написання третього розділу кваліфікаційної роботи, було розроблено інформаційну модель діяльності страхової компанії з подальшим розбиттям її на рівні декомопзиції, та змістове пояснення до них.

Наступним пунктом стала розробка алгоритму захисту персональних данних клієнта, структора якого базується на лінійній алгебрі та матетичне доведення дієздатності алгоритму с подальшою реалізацією на високорівневій об’єктно-орієнтованій мові програмування Pyhton.

В розділі згідно завдання кваліфікаційної роботи, було розроблено Web-ресурс для можливості взаємодії між банками та страховими компаніями. Та ілюстративно зображено основний функціонал роботи ресурсу, з поясненням як він реалізовувався програмно.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1) Капилюк О.І., Музичка О.М. Банківські операції. — К. : Центр учбової літератури, 2012.

2) Румянцев А. Перспективи розвитку банківського страхування // Банкір. — № 1(31). — 2010.

3) Котловський В.С., Неізвестна О.В. Банківські операції: навчальний посібник. — К.: Кондор, 2011.

4) Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. and Saadi, M. (2018). *Big data security and privacy in healthcare: A Review*. [online] www.elsevier.com. Available at: https://reader.elsevier.com/reader/sd/pii/S1877050917317015?token=D846E08C5FCA82A132324DA47B16E00EF7AC2C5A61B478FBE93AEF1CF8078D12C23F10C9A396316D202DF07A27B3FE32

5) Sennaar, K. (2018). *How America's Top 4 Insurance Companies are Using Machine Learning –*. [online] TechEmergence. Available at: https://www.techemergence.com/machine-learning-at-insurance-companies/

6) Snezhana Dichevska, Vera Karadjova, Bank insurance – An Opportunity for Development and Improvement of Financial Market, pp. 385.

7) Szewieczek D., The Risk of Cooperation Between Banks and Insurance Companies, 2013, Studia Ekonomiczne. (127), pp. 137-151.

8) Марр, Б. (2018). *Як великі дані назавжди змінюють страхування* . [онлайн] Forbes. Доступно за адресою: https://www.forbes.com/sites/bernardmarr/2015/12/16/how-big-data-is-changing-the-insurance-industry-forever/#4169df22289b

9) Hawker, A 2000. Безпека та контроль в інформаційних системах: Посібник для бізнесу та бухгалтерського обліку в Інтернеті.

10) Герц, М., Гулдентопс, Е., і Строус, Л. 2001. Цілісність, внутрішній контроль і безпека в інформаційних системах: з'єднання управління та технологічної мережі.