Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

освітній рівень ***магістр***

кваліфікація _____
(назва освітнього рівня)

на тему: Методи захисту персональних даних в системі управління відносинами з клієнтами (CRM-системі)

Виконавець: студент II **курсу, групи** КБМ-21

_____ Швед Анастасія Вадимівна
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Бучик С.С.		

Рецензент	Самохвалов Ю.Я.		

Нормоконтроль			

Київ
2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.

«_____» _____ 2021 року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва напряму підготовки)

студенту КБМ-21 (група) Швед Анастасії Вадимівні (прізвище ім'я по-батькові)

Тема дипломної роботи Методи захисту персональних даних в системі управління відносинами з клієнтами (CRM-системі)

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №2 від 08.10.2020 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДО РОБОТИ

Об'єкт досліджень процеси забезпечення захисту персональних даних при використанні системи управління відносинами з клієнтами.

Предмет досліджень методи захисту персональних даних у системі управління відносинами з клієнтами.

Мета вдосконалення існуючих методів захисту персональних даних в

системі управління відносинами з клієнтами.

Вихідні дані для проведення роботи персональні дані, методи захисту персональних даних в сучасних системах управління відносинами з клієнтами.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна полягає у вдосконаленні існуючих методів захисту персональних даних в системі управління відносинами з клієнтами від ризиків, пов'язаних з людським фактором, та розробці механізму фіксації зміни даних у CRM-системі Creatio.

Практична цінність полягає у створенні нового механізму фіксації змін даних у CRM-системі Creatio, який дозволяє здійснювати фіксацію більшої кількості змін даних, в тому числі на рівні бази даних.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Удосконалення методів захисту персональних даних клієнтів при використанні систем управління відносинами з клієнтами.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	11.10.2020 – 25.11.2020
Аналіз літератури	26.11.2021 – 21.02.2021
Нормативно правове забезпечення	22.02.2021 – 26.02.2021
Аналіз ризик-орієнтованого підходу до захисту персональних даних	01.03.2021 – 05.03.2021
Визначення загроз персональним даним при використанні CRM-систем	08.03.2021 – 12.03.2021
Огляд сучасних CRM-систем	15.03.2021 – 20.03.2021
Огляд методів захисту персональних даних у сучасних CRM-системах на прикладі Creatio	22.03.2021 – 02.04.2021
Реалізація механізму фіксації змін даних у CRM-системі Creatio	05.04.2021 – 30.04.2021
Оформлення пояснювальної записки	03.05.2021 –13.05.2021

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Підготовка до захисту дипломної роботи	17.05.2021 – 26.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект полягає у зменшенні витрат підприємств на вирішення помилок, пов'язаних з помилками та умисними негативними діями користувачів при введені даних у системи управління відносинами з клієнтами.

Соціальний ефект полягає у покращенні стану захищеності персональних даних клієнтів при використанні систем управління відносинами з клієнтами, за рахунок чого підвищується ефективність використання цих систем.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ _____
(підпис) (ініціали, прізвище)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

УДК 004.056.53

РЕФЕРАТ

Пояснювальна записка складається зі вступу, основної частини, що містить 3 розділи, висновків та списку використаних джерел. Загальний обсяг роботи – 94 сторінок. Робота містить 30 рисунків, 4 таблиці та 1 додаток. Список використаних джерел включає 20 джерел.

Об’єкт дослідження: процеси забезпечення захисту персональних даних при використанні системи управління відносинами з клієнтами.

Мета роботи: вдосконалення існуючих методів захисту персональних даних в системі управління відносинами з клієнтами.

Методи дослідження: модель атрибутів безпеки CIA та теорія ризиків за технологією IT-Grundschutz, аналіз методів захисту даних у CRM-системі, тестування розробленого механізму сучасні технології і практики управління інформаційною безпекою на підприємствах різних форм власності.

В основній частині роботи здійснено аналіз існуючих загроз персональним даним клієнтів підприємств, що використовують систему управління відносинами з клієнтами, та визначено ризики, які можуть бути реалізовані через ці загрози. Зроблено висновок, що ключовою загрозою при зберіганні та обробці даних в CRM-системах є людина, а ключовим ризиком – ризик помилкового введення неправильних даних або умисне їх пошкодження.

На прикладі CRM-системи Creatio у роботі досліджено методи захисту персональних даних, які використовуються у сучасних системах управління відносинами з клієнтами. Визначено, що існуючий механізм журналювання змін даних у системі Creatio не покриває всі потреби у здійсненні захисту персональних даних в CRM-системі.

Практичне значення роботи полягає в удосконалені механізму фіксації зміни даних у CRM-системі Creatio.

Наукова новизна полягає у вдосконаленні існуючих методів захисту персональних даних в системі управління відносинами з клієнтами від ризиків, пов’язаних з людським фактором.

У роботі надано рекомендації щодо впровадження удосконаленого механізму у CRM-систему та загальні рекомендації щодо здійснення правил розмежування доступу.

Ключові слова: система управління відносинами з клієнтами, персональні дані, загрози персональним даним, методи захисту персональних даних, багаторівнева архітектура, мікросервісна архітектура, журналювання.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

API – application programming interface
BPM – business process management
BPMN – business process management notation
CAC – customer acquisition cost
CRM – customer relationship management
GDPR – General Data Protection Regulation
HTML – hypertext markup language
IEC – International Electrotechnical Commission
ISO – International Organization for Standardization
LDAP – lightweight directory access protocol
OS – operating system
SQL – structured query language
XML – extensible markup language
XSS – cross-site scripting
БД – база даних
ПЗ – програмне забезпечення
СУБД – система управління базами даних

ВСТУП

Сьогоденне збільшення кількості товарів та послуг призводить до зростання конкуренції серед підприємств та виникнення нових способів утримання конкурентної переваги і збільшення прибутку. Саме тому організації намагаються залучати нових клієнтів та утримувати вже існуючих. Звичайно, зі збільшенням кількості споживачів повинна зростати і кількість менеджерів по роботі з клієнтами, але не всі компанії можуть собі дозволити збільшувати штат відповідно до зростання кількості клієнтів. Це призводить або до зменшення швидкості обслуговування клієнтів, або до зниження якості роботи менеджерів. Обидва варіанти дуже негативно впливають на репутацію підприємства, що зрештою призводить до ще більшого зменшення кількості споживачів товару або послуг та зниження прибутків організації.

Системи управління відносинами з клієнтами призначені для збору, зберігання й аналізу інформації про споживачів, а також для автоматизації споживчих бізнес-процесів, що допомагає персоналу з роботи з клієнтами виконувати свої функції швидше та ефективніше.

Варто зазначити, що зберігання персональних даних клієнтів в єдиному місці є головною перевагою, та в той же час недоліком системи управління відносинами з клієнтами. Відповідно до цього, необхідно розуміти базові можливості системи щодо захисту інформації, яка в ній зберігається та обробляється, щоб побудувати правильний вектор розвитку системи захисту персональних даних у системі управління відносинами з клієнтами.

Розглядати в загальному вигляді технічні методи захисту всіх сучасних CRM-систем неможливо. Єдиним спільним компонентом системи усіх підприємств є співробітник, який працює з персональними даними клієнтів. Саме тому загроза втрати цілісності та конфіденційності персональних даних клієнтів, що зберігаються та обробляються у CRM-системі, шляхом здійснення внутрішнього негативного впливу також дуже велика. В силу наявності у співробітників компанії

безпосереднього доступу до системи, крім умисних дій, існує дуже висока ймовірність введення неправильних даних, або навіть їх видалення.

Основною особливістю підходу до захисту персональних даних в системі управління відносинами з клієнтами є те, що в ній необхідно приділяти більше уваги діям користувачів та швидко реагувати у разі виникнення помилок та інших інцидентів, пов'язаних з модифікацією або видаленням персональних даних клієнтів.

Мета роботи: вдосконалення існуючих методів захисту персональних даних в системі управління відносинами з клієнтами.

Об'єкт дослідження: процеси забезпечення захисту персональних даних при використанні системи управління відносинами з клієнтами.

Предмет дослідження: методи захисту персональних даних у системі управління відносинами з клієнтами.

Задачі, які необхідно вирішити:

– визначити основні загрози та ризики персональним даним у системах управління відносинами з клієнтами;

– визначити існуючі методи захисту даних у системі управління відносинами з клієнтами на прикладі CRM-системи Creatio;

– визначити недоліки існуючих методів захисту системи управління відносинами з клієнтами на прикладі CRM-системи Creatio;

– удосконалити існуючі у CRM-системі Creatio методи захисту даних, а саме реалізувати новий механізми фіксації змін даних.

Наукова новизна полягає у вдосконаленні існуючих методів захисту персональних даних в системі управління відносинами з клієнтами від ризиків, пов'язаних з людським фактором.

Практичне значення роботи полягає в удосконалені механізму фіксації зміни даних у CRM-системі Creatio.

Таким чином, актуальним науковим завданням, що має теоретичне і практичне значення, є удосконалення механізмів фіксації змін даних, внесених

користувачами системи управління відносинами з клієнтами, що покриває всі способи модифікації даних.

РОЗДІЛ 1
ВИЗНАЧЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМАХ УПРАВЛІННЯ ВІДНОСИНАМИ З КЛІЄНТАМИ

1.1 Значення клієнтської бази для сучасних підприємств

Головним завданням будь-якого підприємства є збільшення прибутків та закріплення своїх позицій на сучасному ринку послуг. Жоден сучасний бізнес не може існувати без клієнтів, адже клієнти – це основа існування будь-якого підприємства, від якої залежить досягнення бізнес-цілей, величина прибутку та загалом існування на ринку.

Підприємства витрачають безліч фінансових та людських ресурсів на залучення нових та утримання існуючих клієнтів. Вартість залучення клієнтів розраховується за формулою 1.1, що визначає показник вартості залучення клієнтів до придбання продукту або послуги (CAC, англ. Customer Acquisition Cost) [1].

$$CAC = \frac{MCC + W + S + PS + O}{CA} \quad (1.1)$$

де MCC – загальні витрати на залучення клієнтів (не постійних клієнтів);

W – заробітна плата співробітникам відділу маркетингу;

S – всі витрати на програмне забезпечення, пов’язане з маркетингом та продажами;

PS – будь-яка додаткова професійна послуга в області маркетингу / продажів (дизайнер, консультант тощо);

O – накладні витрати, пов’язані з маркетингом та продажами;

CA – загальна кількість залучених клієнтів.

Проаналізуємо, скільки коштів витрачають підприємства на залучення користувачів на прикладі підприємства monobank та порахуємо їх показник CAC.

Станом на 2020 рік, підприємством було заявлено, що лише за пів року їх клієнтська база стала більшою на 614 000 користувачів [2]. За даними цього ж джерела, штаб monobank'у налічує 2000 співробітників. Скоріше за все, більшість з них є менеджерами по роботі з клієнтами, банківськими спеціалістами, розробниками тощо. Тож припустимо, що від 2000 осіб 5% є співробітниками відділу маркетингу – це 100 людей.

Проаналізувавши ринок праці на відомому ресурсі, бачимо, що середня заробітна плата спеціаліста з маркетингу становить 25 000 грн. Отже в місяць на заробітні плати співробітникам відділу маркетингу підприємство витрачає близько 2 500 000 грн в місяць та 15 000 000 грн за пів року.

До загальних витрат віднесемо рекламу по телебаченню, у мережі Інтернет та біл-бордах. За даними одного інтернет джерела, у 2020 році monobank запустив найбільшу рекламну компанію в своїй історії, в яку входила відео-реклама на телебаченні та в мережі інтернет, та зовнішня реклама на біл-бордах [3].

Компанія відмовилась коментувати бюджет, який було витрачено на цю рекламну компанію, тому розрахунки будуть здійснюватися приблизні. Отже, на цьому ж інтернет-ресурсі зазначено, що зйомки ролику відбувались 2 дні по 15 годин, тож мінімум 30 годин витрачено лише на сам процес зйомки, не беручи до уваги підготовку, написання сценарію тощо. Візьмемо приблизну уявну суму, яка може знадобитись на створення сценарію, підбір та оренду декількох локацій, знімальну команду, візажистів, реквізит, акторів та масовки, монтаж відзнятого матеріалу та отримаємо 450 000 – 500 000 грн.

Також інтернет-видання AIN.UA зазначило, що увесь ролик реклами monobank'у вийшов тривалістю 75 секунд, після чого його було розбито на хронометражі та випущено на телебаченні у форматі тридцяти секундних відео [3]. Крім цього, короткі ролики по 15 секунд транслювалися в якості реклами в інтернет-ресурсі YouTube.

За даними 2019 року вартість секунди реклами на телебаченні варіюється від 1,2 грн до 2829 грн в залежності від каналу та часу доби (ранні години, вечірній прайм-тайм тощо). Візьмемо усереднене значення реклами у вечірній час доби – 850

грн./сек. Припустимо, що протягом півроку рекламу monobank'у показували 120 днів, 5 разів на день по 30 секунд. В результаті отримуємо 15 300 000 грн за рекламу на телебаченні. Оплата реклами на YouTube здійснюється лише за ті рекламні ролики, які не були пропущені користувачами. Візьмемо середню ймовірну вартість реклами в інтернеті – 50 000 грн за місяць та 300 000 за пів року.

Кошти, витрачені на біл-борди та зовнішню рекламу оцінюємо також приблизно. Вартість розробки макету реклами закладаємо у заробітну плату співробітників відділу маркетингу, вартість розміщення реклами на біл-бордах протягом півроку оцінюємо наступним чином: середню вартість оренди зовнішньої реклами по усім містам України (15 000 грн) множимо на ймовірну кількість таких біл-бордів по всій Україні (200) та отримуємо 300 000 грн.

Отже, приблизний показник CAC monobank'у за другу половину 2020 року становить 15 000 000 + 500 000 + 15 300 000 + 300 000 + 300 000 / 614 000 = 51.14 грн.

І хоча результати розрахунків є дуже приблизними, ми бачимо, що для такого підприємства як monobank вартість залучення одного клієнта не є досить високою. Проте переглядаючи загальну вартість рекламної кампанії – близько 31 400 000 грн – можна дійти до висновку, що підприємства витрачають величезні кошти на те, щоб долучити нових клієнтів, а крім цього необхідно ще обслуговувати та утримувати існуючих.

Тож робимо висновок, що клієнтська база є одним з критичних інформаційних активів підприємства, який потребує великих капіталовкладень та дозволяє компанії отримувати прибуток зі своєї операційної діяльності.

1.2 Основні функції сучасних систем управління відносинами з клієнтами

Значення клієнту для сучасного бізнесу дуже велике, тому процес побудови взаємовідносин з клієнтами набуває все більшого значення для розвитку бізнесу, що спонукає створенню ряду програмних продуктів, полегшуючих цей процес.

Управління взаємовідносинами з клієнтами – це широко визнана та застосовувана стратегія управління та підтримки відносин компанії з клієнтами та перспективами продаж [4]. Вона включає в себе використання технологій для організації, автоматизації та синхронізації бізнес-процесів продажів, маркетингу, обслуговування клієнтів та технічної підтримки. Загальні цілі таких систем полягають у пошуку, залученню та завоюванню нових клієнтів, а також утриманні тих, які вже обслуговуються компанією.

Крім вищезазначеного, управління взаємовідносинами з клієнтами визначає загально корпоративну бізнес-стратегію, яка охоплює всі відділи, що працюють з клієнтами, та підвищує прибутковість разом зі зниженням операційних витрат.

Інформаційними системами, що забезпечують ефективну орієнтацію на ринок, наразі являються системи класу CRM (англ. Customer Relationship Management), тобто системи управління відносинами з клієнтами. Системи управління відносинами з клієнтами виступають альтернативним напрямом розвитку маркетингової діяльності підприємств таких галузей як роздрібна та оптова торгівля, здавання в оренду автомобілів, створення програмного забезпечення, медицина, банківська діяльність, виробництво тощо.

На початку свого розвитку CRM-системи існували лише в якості методу автоматизації процесів планування потреб підприємств у виробничих ресурсах та не використовувались для здійснення маркетингових компаній або автоматизації процесів, що потребують складних алгоритмів та мають безліч етапів [5]. Наразі основною задачею CRM-систем є систематизація клієнтських персональних даних та надання користувачам системи доступу до цих даних.

Отже система управління відносинами з клієнтами дозволяє зберігати персональні дані клієнтів у зручному вигляді, забезпечуючи складні зв’язки між ними.

Слід зазначити, що в CRM-системі не завжди зберігаються повністю всі персональні дані клієнтів. Зазвичай, великі підприємства мають декілька систем, в яких здійснюється зберігання тих чи інших даних: наприклад банківські організації частіше за все мають автоматизовані банківські системи типу Б2 (система

автоматизації та оптимізації діяльності банків компанії CS Ltd), в яких зберігається найбільш актуальна інформація, системи обліку банківських операцій тощо. За таких умов CRM-системи виступають в ролі єдиного додатку, що забезпечує користувачам доступ до всіх персональних даних клієнтів з єдиного місця. Це забезпечується можливістю здійснення інтеграцій CRM-системи з іншими вищезазначеними системами підприємства. При цьому дані, отримані з інтегрованих систем, можуть зберігатись у тимчасових таблицях, видалятись після їх використання та не зберігатись безпосередньо в базі даних CRM-системи.

Сучасне уявлення про CRM-системи вже вийшло за рамки інструменту автоматизації продажів та взаємовідносин з клієнтами, адже більшість вендорів все частіше включають у склад своїх програмних продуктів функціональність, що дозволяє здійснювати управління бізнес-процесами BPM (англ. Business Process Management).

Таким чином, сучасні CRM-системи здатні комплексно автоматизувати процеси бізнесу у всіх сферах його діяльності; від процесів продажів, залучення клієнтів, маркетингових компаній до процесів обслуговування клієнтів у банківських структурах, оформлення заявок на отримання кредиту, депозиту, картки, здійснення розрахунку скорингових показників тощо.

Такі CRM-системи також пов’язують функції фронт офісу (наприклад, обслуговування клієнтів) та бек-офісу, тобто допоміжних підрозділів, які здійснюють безпосередню обробку запитів клієнтів (наприклад, верифікацію заявок). Це дозволяє здійснювати ефективну обробку запитів клієнтів, не витрачаючи при цьому час на надсилання запитів поштою чи у роздрукованому вигляді – запити автоматично потрапляють до співробітника, відповідального за його обробку на тому чи іншому етапі процесу.

Головним атрибутом CRM-систем, які поєднують у собі функції BPM, є бізнес-процес – набір дій, які виконуються співробітниками для досягнення певної цілі. Перевагою бізнес-процесів також є те, його учасники можуть не знати послідовність усіх етапів, а виконувати свої функції лише там, де це передбачено логікою процесу.

Для моделювання бізнес-процесів, які автоматизовуються в CRM-системах, використовується система умовних позначень BPMN (англ. Business Process Model and Notation), тобто нотація та модель бізнес-процесів.

Щоб зрозуміти, які функції може виконувати CRM-системи, розглянемо приклад автоматизації процесу у банківській організації: процес розгляду кредитної заявки, поданої через мобільний додаток, який може бути завершений відмовою або підтвердженням.

Приклад змодельованого в нотації BPMN бізнес-процесу можна побачити на рис. 1.1.

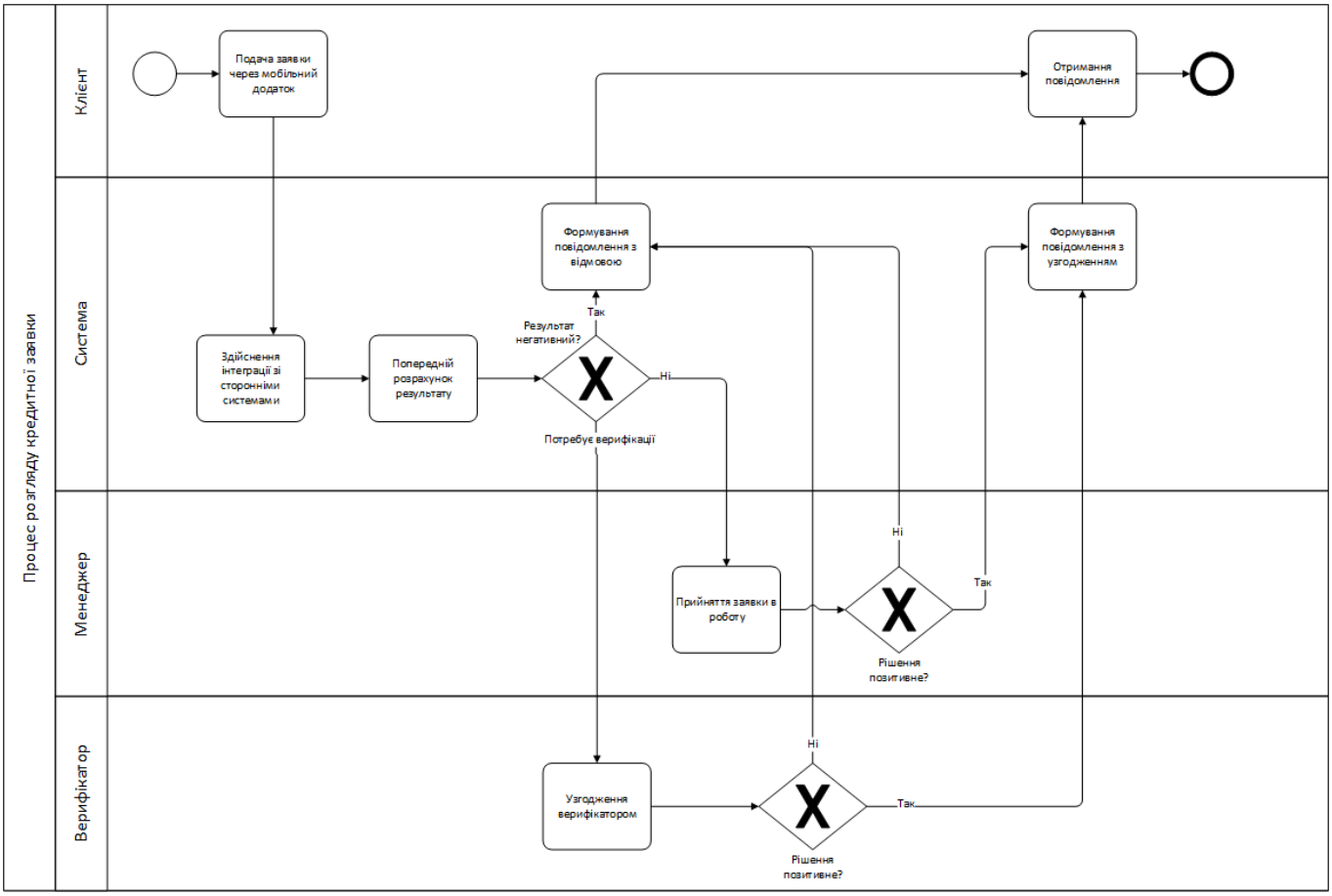

Рисунок 1.1 – Схема бізнес-процесу розгляду кредитної заявки

Як можна побачити на рис 1.1, верифікатору не важливо, які етапи заявка проходить до його узгодження, в нього так само не має необхідності постійно слідкувати за нею – на потрібному етапі йому прийде повідомлення, що заявка потребує його реакції. Також в схему процесу включено додаткові етапи

попереднього розрахунку результату, тож за певних умов змодельований процес відправить відмову клієнту навіть без обробки заявки співробітником банку.

Така автоматизація процесів значно оптимізує робочий час співробітників, мінімізує зайві ітерації між ними та пришвидшує процеси обслуговування клієнтів.

Отже, враховуючи все вищесказане, можна прийти до висновку, що сучасні CRM-системи крім виконання своїх основних функцій – зберігання та обробка обширної клієнтської бази – дозволяють підприємствам автоматизовувати свої процеси, що збільшує швидкість обслуговування клієнтів та позитивно впливає на репутацію та прибутки підприємства.

1.3 Нормативно-правове регулювання питань захисту персональних даних

З точки зору захисту персональних даних в CRM-системах головним інформаційним активом, що підлягає захисту, є персональні дані клієнтів, що обслуговуються цією системою.

Для забезпечення збереження основних властивостей персональних даних клієнтів необхідно застосовувати відповідні міри забезпечення безпеки, які охоплюють великий діапазон загроз та мають на меті зменшення впливу загроз на основні процеси організації та інформаційні активи.

Як вже було зазначено вище, система управління відносинами з клієнтами існує для автоматизації та оптимізації процесів обслуговування клієнтів, шляхом зберігання та оброблення їх персональної інформації. До таких даних можуть відноситися паспортні дані клієнтів, адреса проживання, ідентифікаційний номер та інші відомості про фізичну особу, яка являється клієнтом певного підприємства.

Таким чином, відповідно до закону України «Про захист персональних даних», така інформація підлягає захисту та її обробка можлива лише за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних [6].

При використанні організацією CRM-системи може виникнути питання, як саме здійснюється процес надання згоди на обробку персональних даних. В законі України «Про захист персональних даних» йдеться мова про те, що згода на обробку персональних даних має бути висловлена у письмовій формі або у формі, що дає змогу зробити висновок про її надання [6].

З основним додатком CRM-системи прямо взаємодіє лише співробітник підприємства, тому у момент заповнення персональних даних клієнта, він може не здогадуватись про відсутність поля «Згоден на обробку персональних даних» або таке може навіть не існувати у системі. Таким чином, наявність згоди не завжди буде очевидною, а отже може йти мова про порушення законодавства.

Крім загального визначення питання захисту персональних даних, особливе значення наразі надається питанню захисту персональних даних саме при використанні автоматизованих систем їх обробки, в тому числі і системами управління відносинами з клієнтами. Захист на цьому рівні повинен забезпечуватись відповідно до таких нормативно-правових актів як «Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», закон України «Про захист персональних даних» тощо.

Інші нормативно-правові документи, такі як НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу», ДСТУ ISO/IEC 15408, в якому зазначають критерії оцінювання системи безпеки, регулюють питання відповідності інформаційної системи необхідному рівню забезпечення захисту даних, що зберігаються та оброблюються у системі.

Генеральний регламент захисту персональних даних (англ. General Data Protection Regulation, GDPR) надає такі вимоги до забезпечення безпеки обробки персональних даних:

– забезпечення псевдонімізацію та шифрування персональних даних;

– здатність своєчасно відновлювати доступність персональних даних у разі виникнення фізичного або технічного інциденту;

– здатність забезпечити постійну конфіденційність, цілісність, доступність і стійкість систем і сервісів обробки;

– здійснення регулярного тестування, оцінку та вимірювання ефективності технічних та організаційних заходів щодо забезпечення безпеки обробки [7].

Як описано вище, одним із зазначених засобів безпеки, відповідно до GDPR, є псевдонімізація – представлення даних таким чином, щоб їх неможливо було віднести до конкретної особи [7].

У загальному вигляді, регламентом GDPR визначається дві категорії даних:

– пряма інформація, що являє собою підкатегорію даних, яка дозволяє напряму ідентифікувати людину (наприклад, ім’я, прізвище, індивідуальний податковий номер тощо);

– псевдонімні дані, що являють собою підкатегорію даних, яка дозволяє виділяти індивідуальну поведінку без безпосередньої вказівки на суб’єкта даних (наприклад, ідентифікатор файлу cookie, хешована електронна пошта, ідентифікатор пристрою тощо).

Тобто псевдонімні дані самі по собі не дозволяють ідентифікувати конкретну особу, але дають змогу виділити таку людину із групи осіб, зокрема на основі таких ідентифікаторів як IP-адреса, ідентифікатори файлів cookie.

Відповідно до GDPR, псевдонімізація персональних даних може знизити ризики для суб'єктів даних та допомогти контролерам та процесам виконати свої зобов’язання по захисту даних. Це пояснюється тим, що псевдонімізація передбачає обробку персональних даних таким чином, що вони більше не можуть бути віднесені до конкретного суб’єкту даних без використання додаткової інформації. При цьому така додаткова інформація повинна зберігатись окремо та підлягати технічному та організаційному захисту, щоб особисті дані не були віднесені до ідентифікованої фізичної особи.

Вимога здійснення регулярного тестування, оцінки та вимірювання ефективності технічних та організаційних заходів щодо забезпечення безпеки обробки повинна враховувати ризики, пов’язані з обробкою даних, зокрема ризики випадкового або умисного видалення, втрати, зміни, несанкціонованого розкриття

або отримання доступу до персональних даних. Лише за виконання цих умов, відповідно до регламенту GDPR, підприємства матимуть змогу надати коректну оцінку достатності рівня безпеки даних, що зберігаються та обробляються у системі.

Оцінка рівня достатності захисту може бути визначена шляхом оцінки системи, в якій персональні дані обробляються та зберігаються, на основі критеріїв відповідно до стандарту ISO/IEC 15408.

Стандарт ISO/IEC 15408 має назву «Загальні критерії безпеки інформаційних технологій» (далі – Загальні критерії) та зазначає критерії оцінки захищеності інформації, яка обробляється в комп'ютерних системах від несанкціонованого доступу, та загальні критерії оцінювання системи безпеки.

Документ містить два основних види вимог безпеки: функціональні, які пред’являються до функцій безпеки та механізмів, які їх реалізують, а також вимоги довіри, які пред’являються до технологій та процесу розробки та експлуатації.

Стандарт «Загальні критерії» використовує таку ієрархію вимог:

- клас – визначає найбільш загальне групування вимог;
- сімейство – групує вимоги в межах класу за певними нюансами;
- компонент – мінімальний набір вимог;
- елемент – вимоги, які визначаються отремо та є самодостатніми.

На Рисунку 1.2 зображено те, як стандарт ISO/IEC 15408 визначає взаємозв’язок понять безпеки.

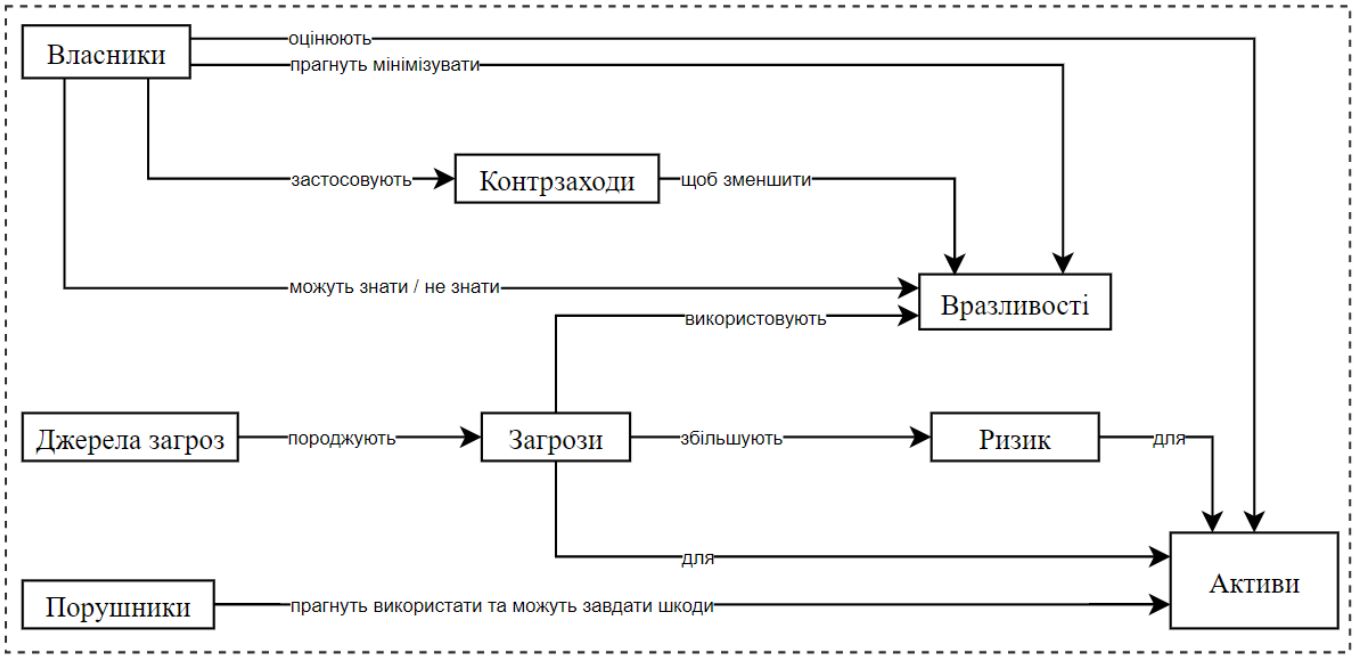

Рисунок 1.2 – Взаємозв’язок понять безпеки за ISO/IEC 15408

В 2017 році в Україні було прийнято всі три частини стандарту ISO/IEC 15408 та опубліковано в якості ДСТУ:

– ДСТУ ISO/IEC 15408-1: ISO/IEC 15408-1-2017 "Інформаційна технологія. Методи й засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 1. Введення й загальна модель";

– ДСТУ ISO/IEC 15408-2: ISO/IEC 15408-2-2017 "Інформаційна технологія. Методи й засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 2. Функціональні компоненти безпеки";

– ДСТУ ISO/IEC 15408-3: ISO/IEC 15408-3-2017 "Інформаційна технологія. Методи й засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 3. Компоненти Довіри".

Для здійснення захисту персональних даних в системах управління відносинами з клієнтами першочергово необхідно визначити:

а) типи актуальних загроз персональним даним, що зберігаються та обробляються у CRM системі;

б) категорію персональних даних, що зберігаються та обробляються у CRM-системі;

в) категорію та рівень знань осіб, що працюють з цими персональними даними.

Відповідно до цих параметрів здійснюється процес управління ризиками інформаційної безпеки, пов'язаними з порушенням основних властивостей інформації, що становить персональні дані, та властивостей самої системи управління відносинами з клієнтами.

Категорія персональних даних, які зберігаються та обробляються у CRM-системі, визначається залежно від конкретного підприємства, так само як і категорія та рівень знань осіб, що працюють з цими персональними даними. Основною цільовою аудиторією CRM-систем є підприємства, які займаються продажом товарів та послуг, залученням та веденням клієнтів. Враховуючи цей факт, можна припустити, що рівень обізнаності у інформаційній безпеці та інформаційних технологіях звичайних менеджерів з продажу зазвичай не задовольняє тому рівню, що дозволяє мінімізувати ризики введення помилкових даних або виконання неприпустимих з точки зору безпеки дій.

Що стосується переліку актуальних загроз, не дивлячись на їх різноманітність, виділити основний перелік загроз персональним даним, що зберігаються та обробляються у CRM-системі цілком можливо. Тож у наступних розділах буде визначено цей перелік та надано рекомендації щодо мінімізації ризиків, яких вони можуть завдати.

1.4 Ризик-орієнтований підхід до захисту інформації

Підходити до питання забезпечення інформаційної безпеки персональних даних необхідно комплексно – впроваджувати політики безпеки та посадові інструкції, що регламентують роботу користувачів, використовувати технічні та апаратні засоби захисту, здійснювати журналювання користувацьких дій та, звичайно, забезпечувати належний фізичний захист.

Здійснення такого комплексно захисту потребує великих фінансових та людських ресурсів, які у підприємств зазвичай обмежені. Зважаючи на це, у питанні

забезпечення інформаційної безпеки підприємства мають визначити та виділити найбільш критичні з точки зору бізнес-процесів ризики та в першу чергу протидіяти їм.

Для цього, відповідно до міжнародних стандартів у сфері інформаційних технологій та інформаційної безпеки, при розробці системи управління інформаційною безпекою підприємствами використовується ризик-орієнтований підхід, що дозволяє визначити рівень ризику, визначити пріоритети та здійснити процес обробки ризику відповідно до найбільш критичних ризиків.

Отже процес аналізу та оцінки ризиків є найважливішим початковим етапом у реалізації інформаційної безпеки підприємства. Управління ризиками дозволяє підприємству встановити основи для інформаційної безпеки та визначити пріоритетні цілі захисту, що ґрунтуються на визначенні найбільш важливих ризиків.

Вигоди використання ризик-орієнтованого підходу можна коротко виразити таким чином:

– скорочення витрат на забезпечення виробництва в середньостроковій і довгостроковій перспективі;

– скорочення вартості втрат на відновлення активів;

– готовність до збоїв у роботі підприємства і його окремих процесів;

– підвищення репутації підприємства [8].

Міжнародний стандарт ISO/IEC 27001 зосереджений на захисті основних властивостей інформації підприємства: конфіденційності, цілісності та доступності. Дотримання цих трьох основних аспектів інформаційної безпеки реалізується шляхом визначення потенційних проблем інформаційним ресурсам та активам (тобто оцінки ризиків) та, на основі них, визначення необхідних шляхів, методів та засобів для попередження виникнення цих проблем (тобто обробка ризиків). Відповідно до цього, головною ідеологією міжнародного стандарту ISO/IEC 27001 є процес управління та аналізу ризиками, який полягає в оцінці ризиків та їх обробці: визначенні допустимого рівня ризику організації та, в подальшому, зменшенні, прийнятті, уникненні або перенесенні ризику, який перевищує допустимий рівень.

Наявність та величина ризиків визначає вимоги до захисту інформаційних активів та засобів, які будуть для цього використані.

Ризик-орієнтований підхід до захисту інформаційних активів підприємства передбачає здійснення комплексного підходу до оцінки, контролю та моніторингу всіх типів ризиків активам підприємства [9]. Крім цього, управління ризиками дозволяє підприємству встановити основи для інформаційної безпеки компанії та визначити пріоритетні цілі захисту, що ґрунтуються на визначенні найбільш важливих ризиків. І хоча загальний підхід до застосування ризик-орієнтованого підходу однаковий у всіх методологіях, міжнародні стандарти надають свої рекомендації до здійснення процесу управління ризиками.

Відповідно до методології IT-Grundshutz, управління ризиками здійснюється за такими етапами:

а) розробка процедури з ідентифікації ризиків;

б) ідентифікація і ранжування активів за каталогом «Модулі» методики IT-Grundschutz;

в) визначення відповідальних за активи;

г) оцінка активів;

ґ) ідентифікація загроз та вразливостей активів за каталогом «Загрози»;

д) розрахунок і ранжування ризиків;

е) розробка плану зі зниження ризиків за каталогом «Заходи захисту» методики IT-Grundschutz

є) визначення непридатних контролів (напрямів) безпеки;

ж) розробка положень з застосування контролів [10].

Відповідно до методології управління інформаційними технологіями COBIT. процес аналізу ризиків починається з оцінки IT-ресурсів підприємства, визначення вразливостей та відповідних їм загроз. Весь процес зображено на рис. 1.3.

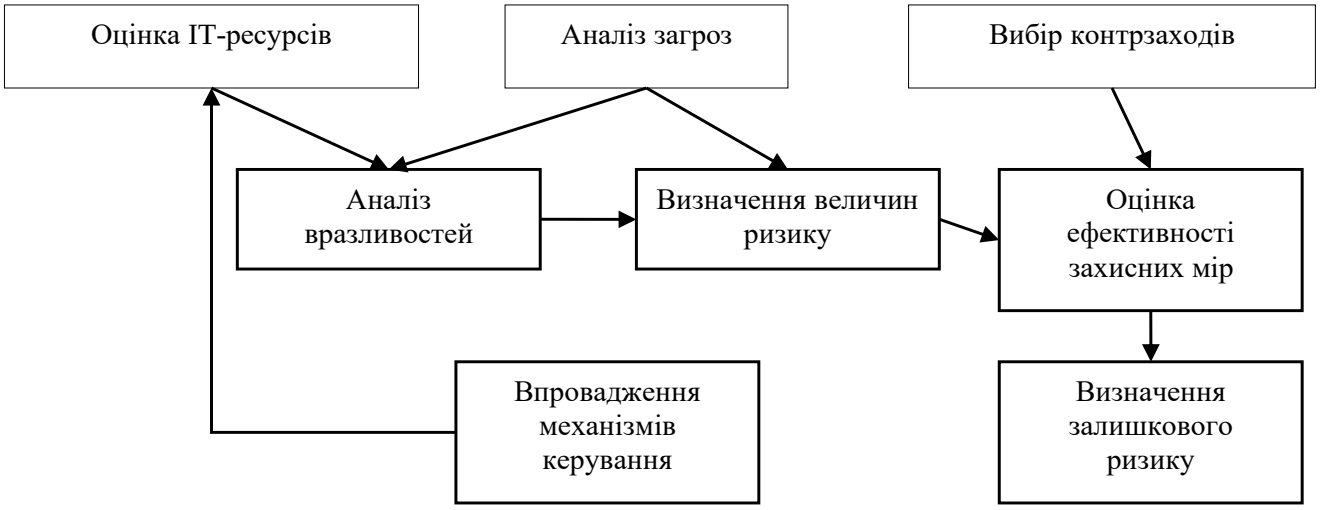

Рисунок 1.3 – Процес аналізу ризиків відповідно до методології COBIT

Отже, як можна побачити, першочерговим етапом в процесі ризик-менеджменту у всіх зазначених методологіях є управління активами підприємства. Він включає в себе процедуру визначення та документування особливо важливих інформаційних активів підприємства – тих, які є необхідними для забезпечення роботи підприємства. До переліку такого роду активів включають не лише інформацію, а і засоби, якими вона оброблюється або передається, персонал, який працює з цими даними, а також будівлю і приміщення, в яких ця інформація циркулює [11].

Процедура ризик-менеджменту дозволяє прорахувати можливі негативні впливи такого роду загрози, розробити необхідні засоби та заходи протидії відповідно до тієї кількості фінансових, часових та людських ресурсів, які має підприємство.

Відповідно міжнародного стандарту NIST 800-30 «Risk management guide for information technology systems» [12] ризик втрати інформаційного активу розраховується за формулою (1.2):

$$\boldsymbol{R = P * W} \tag{1.2}$$

де R – ризик інформаційному ресурсу,

P – ймовірність реалізації загрози,

W – кількісна оцінка вартості реалізації загрози на ресурс.

Точно розрахувати ймовірність виникнення загрози або збиток від інциденту майже неможливо, оскільки на ці величини зазвичай впливає дуже багато факторів. Проте навіть з формули 1.2 можна зробити висновок, що ризик порушення захисту такого активу як персональні дані клієнтів підприємства прямо пропорційний ймовірності реалізації загрози та вартості активу, який в даному випадку вимірюється коштами, витраченими на залучення клієнтів.

Слід зауважити, що кошти – це не єдині втрати, які може понести підприємство у разі викрадення або пошкодження персональних даних клієнтів, що обслуговується організацією.

Безліч факторів, такі як глобалізація, економічна та культурна відкритість, розповсюдження глобальних компаній по всьому світі і багато інших призводять до зростання конкуренції між компаніями. В результаті ми бачимо, що, з одної сторони, виникає все більше безлічі продуктів та послуг від різних виробників, а з іншої, продукти, що відносяться до однієї категорії, існують в такому великому різноманітті, що часом пропозиція перевищує попит.

Саме тому репутація підприємства є не менш важливим активом, який може приваблювати, або навпаки відштовхувати нових клієнтів. У разі виникнення хоча б одного інциденту, пов’язаного з витоком даних або неможливістю отримання інформації у той час, коли клієнту це необхідно, споживач послуги з меншою ймовірністю захоче далі співпрацювати з організацією, яка це допустила.

Розуміючи, що клієнти – це основа існування будь-якого підприємства, від якої залежить досягнення бізнес-цілей, величина прибутку та загалом існування на ринку, компанії все більше замислюються над автоматизацією процесів обробки персональних даних клієнтів та їх захисту.

Крім всього вищезазначеного, існує ряд стандартів та нормативно-правових документів, які регулюють захист персональних даних клієнтів на державному та міжнародному рівнях. Тому підприємства, які безпосередньо співпрацюють з персональними даними фізичних та юридичних осіб, повинні налаштовувати свої процеси з урахуванням вимог нормативних документів.

1.5 Загрози персональним даним при використанні CRM-систем

Для багатьох сучасних компаній клієнтська база є головним активом, а система взаємодії з клієнтами, в свою чергу, є однією з інформаційних систем керуючого ядра компанії і однією з найцінніших систем, оскільки саме в ній розміщена інформація, що дозволяє компанії отримувати прибуток зі своєї операційної діяльності. Тому CRM-системи компанії є об'єктами атак як зовнішніх хакерів, так і недобросовісних співробітників компанії, які можуть виступати в ролі інсайдерів.

Великий ризик виникнення внутрішніх загроз з боку співробітників пояснюється наявністю єдиної точки доступу до великої кількості персональних даних, що являє собою велику небезпеку втрати конфіденційності або цілісності цієї інформації.

Дарма можна подумати, що персональні дані клієнтів являють собою не таку привабливу здобич, як, наприклад, комерційна таємниця підприємства, яка може містить таємні алгоритми, програми, схеми тощо. Тому власники систем управління відносинами з клієнтами можуть марно сподіватись, що захищати персональні дані клієнтів не має необхідності, мовляв, кому може знадобитись дата народження, мобільний телефон чи місто проживання клієнта). Проте для продажів, на яких покладено основну частину прибутку підприємств, дуже затребувано та «привабливо» виглядає навіть проста клієнтська база, тому наповнення CRM-системи може цікавити зловмисників з таких причин:

– видалення клієнтської бази конкурентів призведе до великих фінансових втрат з її боку, та втрати репутації, що може зіграти на руку компанії-конкуренту;

– співробітники, що виступають в ролі інсайдерів, можуть при звільненні з підприємства (або навіть працюючи в ньому) продавати клієнтську базу з ціллю власної наживи;

– персональні дані самих співробітників можуть бути використані компаніями-конкурентами з використанням методів соціальної інженерії.

Крім цього, сучасні CRM системи можуть містити дані щодо продуктового каталогу підприємства, що теж стане цікавою здобиччю для конкурентів, та інформаційну базу даних співробітників, яку можна використати у соціальній інженерії. Також клієнтська база може мимоволі стати ціллю «хакера-любителя», який захоче отримати доступ до БД заради перевірки своїх здібностей, або заради цікавості. Реалізована атака на CRM систему може завдати як фінансових, так і репутаційних негативних наслідків.

Отже, відповідно до причин, за яких здійснюється розкрадання чи пошкодження даних, що зберігаються у CRM системах, основними загрозами, визваними умисними діями, можуть бути:

– сторонні зловмисники, хакери, компанії-конкуренти;
– інсайдери.

Звичайно, що така інформація, як продуктовий каталог або секретні алгоритми можуть бути дуже корисними для компаній-конкурентів, але головну роль у крадіжці інформації грають інсайдери. До того ж, це не обов'язково лише ті співробітники, які працюють у штабі у цей час, це можуть бути і колишні співробітники, партнери, співробітники суміжних підрозділів, які мають доступ до інформації, яку безпосередньо не використовують у своїй роботі.

Резюмуючи все вищесказане, до головних загроз інформаційній безпеці бізнесу при використанні CRM систем можна віднести:

– неприпустимі дії співробітників;
– втрата даних клієнтів;
– атаки на роботу системи;
– низька якість ПО;
– шахрайство з електронними документами;
– крадіжка конфіденційної інформації.

Verizon Data Breach Investigations Report – це щорічне видання, яке здійснює аналіз інцидентів інформаційної безпеки з особливим акцентом на питання витоку даних. Звіт Verizon Data Breach Investigations Report від 2020 року надає статистику

[13] розкрадання даних компаній з точки зору об’єкту виникнення інцидентів (рис. 1.4):

Рисунок 1.4 – Аналіз жертв інцидентів інформаційної безпеки за 2020 р.

Як ми бачимо на рис. 1.4, у більше половини жертв було зафіксовано факт отримання несанкціонованого доступу до захищених персональних даних. При цьому 72% порушень припадає на великі підприємства, яким витік конфіденційної інформації може значно підірвати репутацію, що негативно вплине на прибутки та залучення нових клієнтів. Такі показники не дивні в 2020 році, адже через пандемію більшість компаній за можливості перенесли процеси надання своїх послуг в онлайн. Оплата послуг в мережі Інтернет передбачає передачу даних платіжних карток, що значно посилило інтерес зловмисників та спроби компрометації цих даних.

Пандемія також змусила багато підприємств перевести співробітників на віддалену роботу, що знизило контроль за їх діями, тож все більше атак були учинені з використанням фішингових атак, соціальної інженерії.

Статистика по порушникам інформаційної безпеки персональних даних зображена на рис. 1.5.

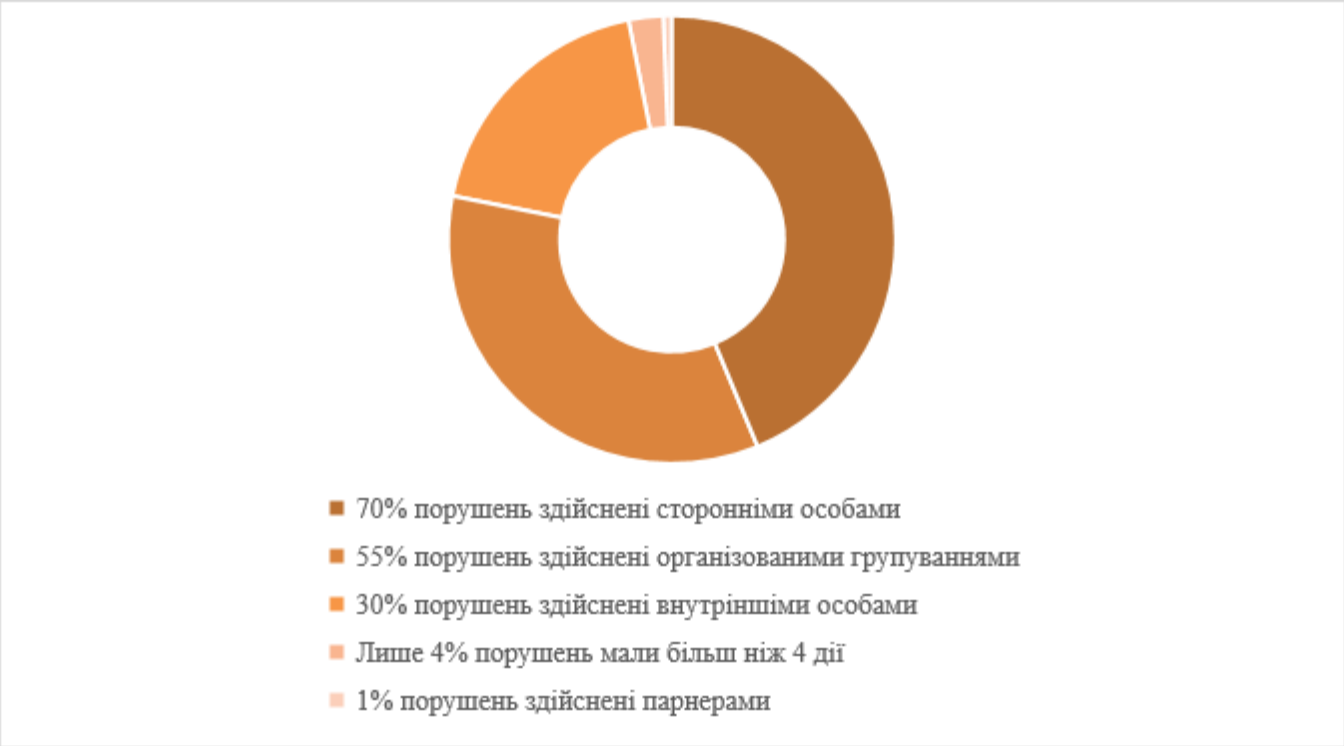

Рисунок 1.5 – Аналіз порушників інцидентів інформаційної безпеки за 2020 р.

Показних порушень, здійснених сторонніми особами дуже великий – 70%, проте і 30% – показник порушень, здійснених внутрішніми особами, – достатньо великий, враховуючи те, що співробітники тих самих CRM-систем мають доступ до персональних даних клієнтів, що в ній зберігаються та обробляються. Як було зазначено раніше, сучасні CRM-системи передбачають роботу користувачів у звичайному браузері, а отже з виходом до мережі Інтернет. За часи роботи в офісах на робочих місцях співробітників можна було проконтролювати встановлення та оновлення антивірусного ПЗ та інших програмних засобів попередження атак на систему. Зараз, коли все більше підприємств підтримують віддалену роботу, в наслідок чого співробітники вимушені використовувати часом навіть власні персональні комп'ютери, це проконтролювати стало майже неможливо. Це пояснює такий високий показник порушень, здійснених внутрішніми особами.

До речі, переглядаючи статистику цього ресурсу за 2017 рік [14], зображену на рис. 1.6 можна побачити, що за 2020 рік кількість зовнішність порушників зменшилась на 5%, натомість кількість внутрішніх порушників зросла на 5%.

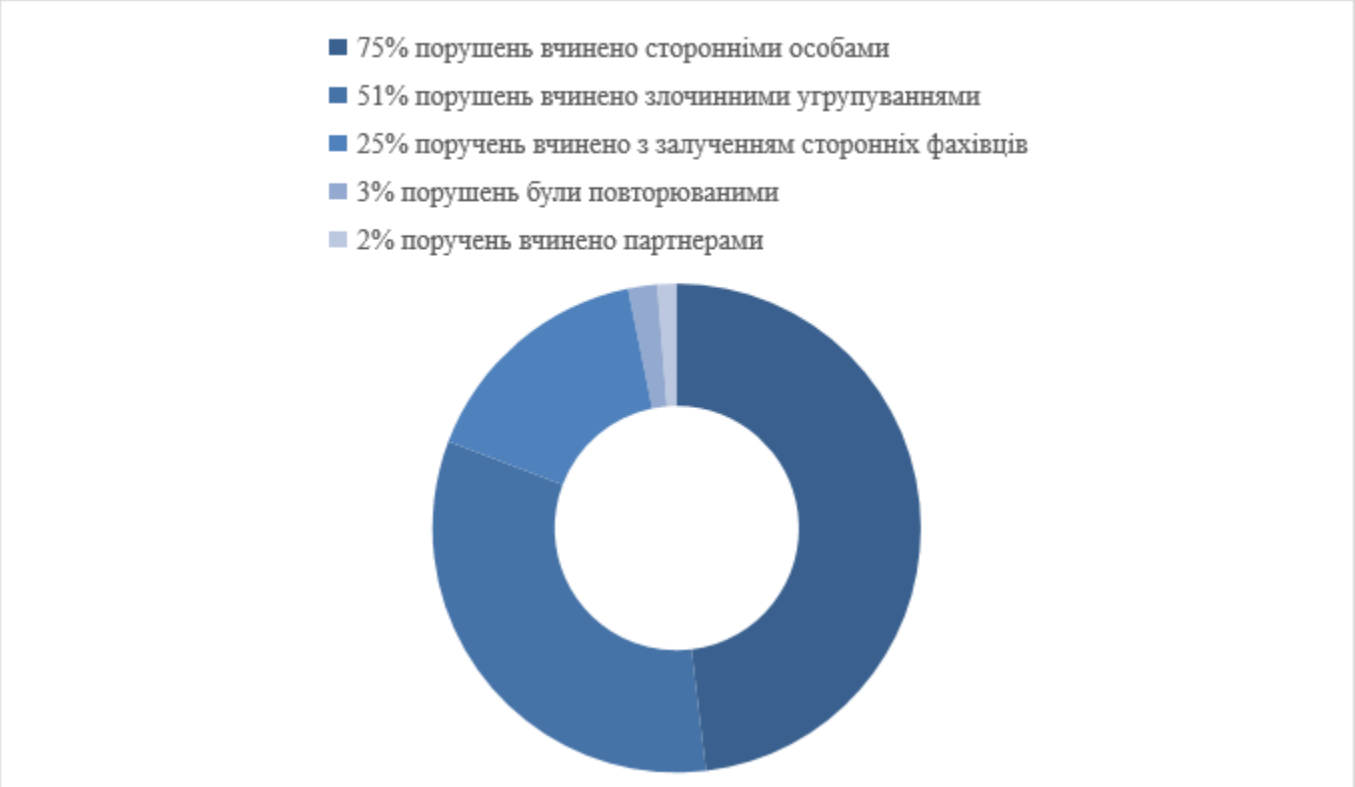

Рисунок 1.6 – Аналіз порушників інцидентів інформаційної безпеки за 2017 р.

Для протидії та попередження загрозам, крім їх джерел необхідно також визначити фактори, які призводять до їх виникнення. До порушень, вчинених сторонніми особами зазвичай відносяться такі дії, як DDoS атаки, злам паролів, завантаження шкідливого ПЗ, фішинг, перехоплення та аналіз мережевого трафіку.

Дії інсайдерів певним чином відрізняються, адже їм не потрібно якось намагатись отримати доступ до конфіденційної інформації, вони вже його мають. Різниця також в тому, що з боку сторонніх порушників майже ніколи не йдеться мова про ненавмисні дій, в той час як пошкодження або навіть видалення даних внутрішніми співробітниками нерідко являється наслідком звичайних помилок.

Компанією Verizon надається ще одна статистика за 2020 рік (рис. 1.7), яка відображає методи, засоби та чинники, які призвели до виникнення інцидентів інформаційної безпеки персональних даних минулого року.

Рисунок 1.7 – Аналіз методів та засобів здійснення інцидентів інформаційної безпеки за 2020 р.

На рис. 1.7 видно, що 22% інцидентів викликані помилками, ще 8% пов’язані зі зловживанням привілеїв авторизованими користувачами. Тож загалом 30% інцидентів інформаційної безпеки були викликані помилками або умисними діями користувачів, що вказує на високий рівень впливу людського фактору на процеси забезпечення інформаційної безпеки та питання захисту персональних даних від несанкціонованого доступу до них.

Ще одним показником, що підтверджує вищесказане твердження, є відсоток порушень, які були здійсненні з використанням соціальних атак – 22%. Така кількість інцидентів, пов’язаних з реалізацією атак методом соціальної інженерії, свідчить про те, що більшість користувачів або є недостатньо обізнаними у питаннях інформаційної безпеки, або співробітники підприємств не зацікавленні у забезпеченні захисту даних, якими вони оперують.

Відсоток порушень, викликаних шкідливим програмним забезпеченням, на думку автора цієї роботи також пов’язаний з тим, що користувачі нехтують правилами відвідування підозрілих сайтів та не користуються антивірусним ПЗ.

Натомість у 2017 році статистика використовуваних методів та засобів реалізації інцидентів інформаційної безпеки персональним даним надається наступна (рис. 1.8):

Рисунок 1.8 – Аналіз методів та засобів здійснення інцидентів інформаційної безпеки за 2017 р.

Порівнюючи статистику використовуваних методів порушення інформаційної безпеки у 2020 (рис. 1.7) та 2017 роках (рис. 1.8) ми бачимо, що відсоток порушень, пов’язаних з шкідливим ПЗ, у 2020 році зменшився майже втричі, а атаки методами соціальної інженерії з 43% зменшились до 22%, натомість величина помилок та зловживання привілеями авторизованих користувачів зросла удвічі, що свідчить про зростаючий ризик порушення інформаційної безпеки через реалізацію загроз, спричинених людським фактором.

Проаналізувавши статистику інцидентів інформаційної безпеки з особливим акцентом на питання витоку даних, можна зробити висновок, що більшість з описаних порушень є наслідками людських дії та помилок, які достатньо складно передбачити при розробці будь-якої системи.

Можна зробити висновок, що загроза втрати цілісності та конфіденційності персональних даних клієнтів, що зберігаються та обробляються у CRM-системі, шляхом здійснення внутрішнього негативного впливу також дуже велика. В силу наявності у співробітників компанії безпосереднього доступу до системи, крім умисних дій, існує дуже висока ймовірність введення неправильних даних, або навіть їх видалення.

В першу чергу високий ризик прояву загроз спричинених користувачами CRM-системи пояснюється тим, що працівниками, які взаємодіють з системою, зазвичай є менеджери підприємств. Не зважаючи на те, що у сучасному світі на кожному кроці спостерігається глобальна інформатизація суспільства, деякі співробітники можуть не мати достатніх знань у сфері інформаційних технологій.

Слід також взяти до уваги, що через зростаючу конкуренцію на ринку надання продукції та послуг, керівництва підприємств прагнуть вдосконалювати процеси обслуговування клієнтів часом впроваджуючи нові і нові рішення надто швидко, не даючи співробітникам адаптуватись до нових систем та повністю в них розібратись.

В кінцевому випадку недостатня обізнаність та недолік часу на вивчення нової системи призводить до виникнення великої кількості помилок під час обробки даних.

1.6 Модель CIA системи стандартизації ISO/IEC

Міжнародний стандарт ISO/IEC 27001 спирається на стандартну модель безпеки – CIA (Confidentiality, Integrity, and Availability – конфіденційність, цілісність і доступність). Ця модель з трьох складових є загальновизнаною при оцінці ризиків, пов'язаних з критичною інформацією, і при затвердженні плану інформаційної безпеки. Поняття «захисту інформації» трактується міжнародним стандартом як «збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені і інші властивості, такі як справжність, неможливість відмови від авторства, достовірність» [15].

Нижче модель CIA описана більш детально:

Конфіденційність. Ця властивість полягає у тому, що критична інформація повинна бути доступна тільки обмеженому колу осіб. Неправомірна передача і використання інформації повинні бути заборонені.

На прикладі CRM-систем втрата конфіденційності персональних даних полягає у розголошенні інформації, наданої клієнтом, стороннім особам. Наприклад, розміщення цих даних на сайті і цілях реклами, без згоди самого клієнта

Цілісність. Властивість інформації, яка полягає у тому, що інформація не може бути модифікована без дозволу її власника, а зміни інформації, що призводять до її втрати чи руйнування, повинні бути заборонені.

На прикладі CRM-систем втрата цілісності персональних даних полягає у їх зміні. Частіше за все на практиці зустрічаються випадки, коли така інформація, надана клієнтом, була спотворена ненавмисно. Наприклад, користувачами CRM-системи досить часто є співробітників контакт-центру. Клієнт може зателефонувати до підприємства, менеджер по роботі з клієнтами по телефону буде вносити певну інформацію щодо цієї особи та, наприклад, здійснить помилку у прізвищі клієнта. Наступний раз, коли ця людина прийде вже у відділення магазину або банку, його не зможуть ідентифікувати за цим прізвищем. В поганому випадку менеджер відділення створить дубль цього клієнта у системі, що негативно буде позначатись на завантажені баз даних CRM-системи підприємства, в гіршому – клієнту відмовлять в обслуговуванні, що призведе до втрати клієнта та погіршення репутації бізнесу.

Доступність. Властивість інформації, яка гарантує, що авторизовані користувачі отримають необхідну їм інформацію в обумовленому часовому інтервалі.

В CRM-системі прикладом втрати доступності персональних є неможливість менеджера надати послуги клієнту через відсутність доступу до баз даних або видалення інформації про клієнта, яка є необхідної для його обслуговування. Ще один приклад: системному аналітику необхідно скласти технічне завдання для адаптації CRM-системи під потреби замовника. Він очікує переліг вимог від замовника, які повинен передати йому бізнес аналітик, який, в свою чергу, з

невідомих причин не може зробити цього. Як результат – вимог немає, технічного завдання немає, розробник не може приступити до корегування системи, замовник не може вчасно отримати продукт, а підприємство втрачає клієнта та гроші. Інформація, необхідна системному аналітику, (вимоги замовника) була недоступна, звідси й невиконання обов'язків та вплив на загальний бізнес-процес

Для забезпечення інформаційної безпеки підприємства, а саме збереження основних властивостей інформації (рис. 1.9) необхідно застосовувати відповідні міри забезпечення безпеки, які мають на меті зменшення впливу загроз на основні процеси організації та інформаційні активи.

Рисунок 1.9 – Основні властивості інформації згідно моделі CIA

Отже в основі моделі CIA лежить принцип захисту основних властивостей інформації: конфіденційності, цілісності та доступності, дотримання якого гарантує ефективність роботи бізнесу та безпеку інформаційних ресурсів і активів.

Система забезпечення захисту персональних даних у CRM-системі нерідко також включає в себе організаційні заходи, політики, процедури, процеси, технічні та програмні засоби захисту, які повинні корелювати з загальної системою управління інформаційної безпеки всього підприємства.

1.7 Оцінка ризиків персональним даним у системах управління відносинами з клієнтами

Процес управління ризиками дозволяє підприємству встановити основи для інформаційної безпеки компанії та визначити пріоритетні цілі захисту. Тому здійснювати всі подальші дії та заходи з забезпечення безпеки персональних даних клієнтів слід лише після чіткого визначення ризиків інформаційним активам.

Першочерговим завданням, яке повинно бути виконано до етапу оцінки ризиків, є визначення важливих для бізнесу активів. Під поняттям «актив» в даному випадку варто розуміти все, що має цінність для підприємства та є важливим для роботи бізнесу. З точки зору інформаційної безпеки достатньо обмежитися лише інформаційними активами – матеріальними або нематеріальними об'єктами, які є інформацією або містять інформацію, або є необхідними для обробки інформації.

Методологією IT-Grundschutz, розробленою федеральним відомством з інформаційної безпеки Німеччини, пропонується згрупувати всі активи підприємства у наступні модулі:

– загальні аспекти, наприклад:
    1) персонал відділу інформаційної безпеки, персонал відділу технічної підтримки, менеджери по роботі з клієнтами тощо (з тієї точки зору, що вони володіють конфіденційною та комерційною інформацією);
    2) персональні дані співробітників, які можуть бути використані для застосування методів соціальної інженерії;
    3) персональні дані клієнтів;
– інфраструктура, наприклад:
    1) будівля;
    2) приміщення, в якому працюють кінцеві користувачі;
    3) серверна кімната;
    4) електричні кабелі;
– IT-системи, наприклад:
    1) сервери;

2) робочі місця користувачів;

3) операційні системи;

4) міжмережеві екрани;

5) комутатори та маршрутизатори;

6) багатофункціональні пристрої, на яких може роздруковувати конфіденційна інформація;

– мережа, наприклад:

1) Інтернет, з точки зору забезпечення фільтрації трафіку, який надходить із-зовні та передається у глобальну мережу;

2) VPN;

– додатки, наприклад:

1) СУБД;

2) CRM-система.

Отже, для того, щоб визначити ризики, спершу необхідно здійснити опис всі наявних активів підприємства. В даній роботі здійснюється аналіз та удосконалення методів захисту саме персональних даних у CRM-системах, тому в якості інформаційного активу будуть розглянуті такі активи:

– персональні дані клієнтів;

– персональні дані співробітників.

Однією з методик, що пропонує здійснювати аналіз ризику у п’ять етапів є методологія IT-Grundschutz. Першим етапом, відповідно до визначеного стандарту, є створення огляду всіх можливих загроз активам.

IT-Grundschutz Catalogues являють собою вичерпний перелік всіх можливих активів компанії та відповідних їм загроз [10]. В каталозі загрози об’єднані в шість наступних груп:

– основні загрози;

– форс-мажорні обставини;

– організаційні недоліки;

– людські помилки;

– технічні несправності;

– умисні дії.

Більш обширно загальну класифікацію загроз інформаційній безпеці підприємства зображено на рис. 1.10.

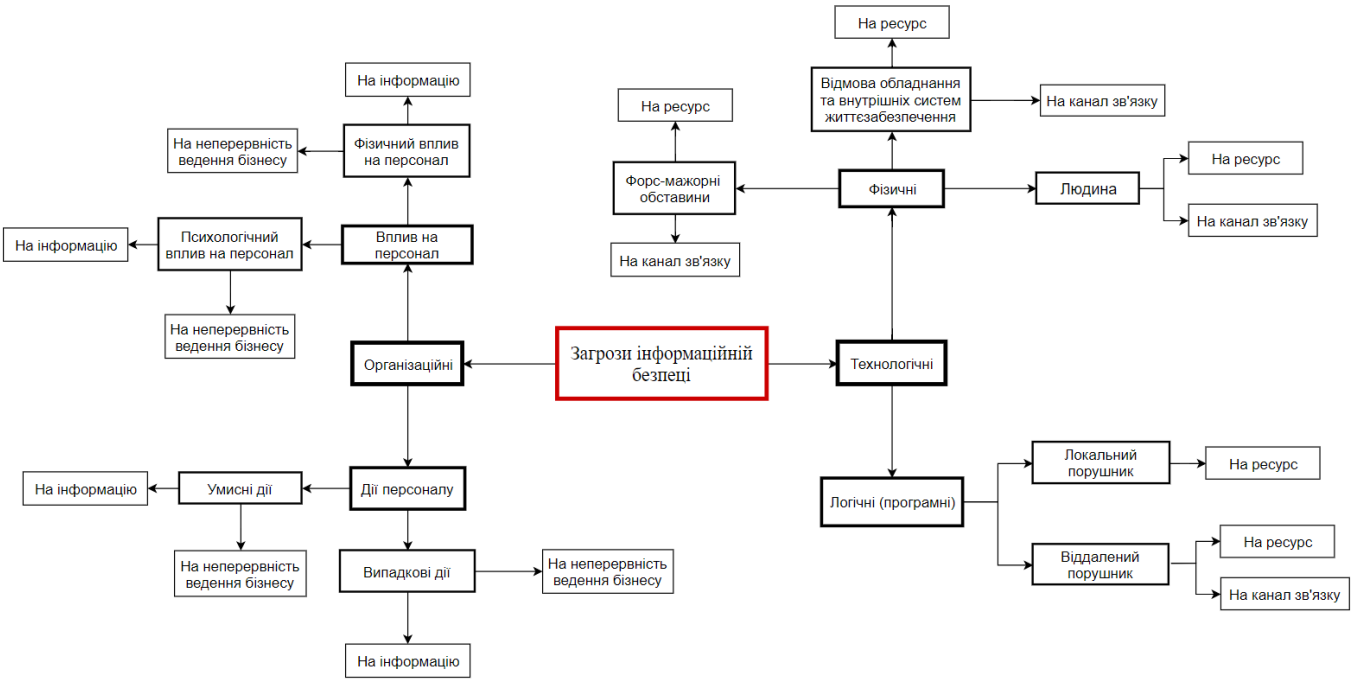

Рисунок 1.10 – Класифікація загроз інформаційній безпеці

Опис ризику за методологією IT-Grundschutz полягає у наступному: вибору активу з каталогу модулів та визначенні загроз активу та вразливостей, через які ці загрози можуть бути реалізовані. Для одного активу можна описати велику кількість ризиків, оскільки активи не обмежуються лише однією вразливістю.

Отже, відповідно до каталогу загроз IT-Grundschutz Catalogues, в даній роботі було ідентифіковано основні загрози персональним даним саме у CRM-системі та представлено у Таблиці 1.1.

Таблиця 1.1

Ідентифіковані загрози персональним даним у CRM-системі

№	Актив	Тип загрози	Загроза
1	Персональні дані клієнтів	Форс-мажорні обставини	Відмова IT-системи або серверів

продовження табл. 1.1

№	Актив	Тип загрози	Загроза
2			Пожежа, потоп
3		Організаційні недоліки	Неправильний порядок зберігання даних
4		Людські помилки	Ненавмисне пошкодження
5			Ненавмисне видалення
6		Технічні несправності	Відмова в обслуговування серверів
7			Пошкодження каналу передачі даних
8		Умисні дії	Крадіжка
9			Пошкодження або знищення
10			Розголошення
11	Персональні дані співробітників	Форс-мажорні обставини	Відмова ІТ-системи або серверів
12			Пожежа, потоп
13		Організаційні недоліки	Неправильний порядок зберігання даних
14		Людські помилки	Ненавмисне пошкодження
15			Ненавмисне видалення
16		Технічні несправності	Відмова в обслуговування серверів
17			Пошкодження каналу передачі даних
18		Умисні дії	Крадіжка
19			Пошкодження або знищення
20			Розголошення

Характеристику цим загрозам з точки зору інформаційної безпеки наведено у Таблиці 1.2 та Таблиці 1.3, які містять такі поля:

– F – частота випадків реалізації загрози за рік,

– P – ймовірність виникнення загрози,

– W – вартість активу в ALE (100 000 грн),

– R – ризик, що розраховується за формулою (1.3).

Ймовірність виникнення загрози розраховується за наступною формулою:

$$P = D : F \qquad 1.3$$

де D – кількість робочих днів в році,

F – частота випадків реалізації загрози за рік.

Таблиця 1.2

Характеристика загроз персональним даним клієнтів у CRM-системі з точки зору інформаційної безпеки

№	Загроза	Вплив			F	P	W	R
		К	Ц	Д				
1	Відмова IT-системи або серверів			+	2	0,008	15	0,12
2	Пожежа, потоп		+	+	1	0,004	14	0,056
3	Неправильний порядок зберігання даних	+	+	+	6	0,024	8	0,192
4	Ненавмисне пошкодження		+		12	0,048	8	0,384
5	Ненавмисне видалення		+	+	10	0,04	10	0,4
6	Відмова в обслуговування серверів			+	9	0,036	16	0,576
7	Пошкодження каналу передачі даних			+	2	0,032	14	0,12
8	Крадіжка	+			3	0,012	11	0,132
9	Пошкодження або знищення		+	+	7	0,028	12	0,336
10	Розголошення	+			6	0,024	11	0,264

Таблиця 1.3

Характеристика загроз персональним даним співробітників у CRM-системі з точки зору інформаційної безпеки

№	Загроза	Вплив			F	P	W	R
		К	Ц	Д				
1	Відмова IT-системи або серверів			+	5	0,02	2	0,04
2	Пожежа, потоп		+	+	1	0,004	2	0,008
3	Неправильний порядок зберігання даних	+		+	9	0,036	4	0,144
4	Ненавмисне пошкодження		+		16	0,064	1	0,064
5	Ненавмисне видалення		+	+	8	0,032	1	0,032
6	Відмова в обслуговування серверів			+	11	0,044	2	0,088
7	Пошкодження каналу передачі даних			+	14	0,056	2	0,112
8	Крадіжка	+			3	0,012	4	0,048
9	Пошкодження або знищення		+	+	6	0,024	2	0,048
10	Розголошення	+			5	0,02	4	0,08

Наведені результати можуть бути використані при здійсненні захисту персональних даних, що зберігаються та оброблюються у CRM-системі, для визначення пріоритетних ризиків, що потребують першочергової обробки.

Алгоритми процесу ризик-менеджменту, наданого міжнародними стандартами серії ISO/IEC 27001 та методологіями IT-Grundschutz і COBIT, після створення реєстру активів, визначення відповідних їм вразливостей, загроз та оцінки ризиків передбачають здійснення експертного підбору критерію прийнятності ризиків[15]. Ризики, оцінка яких перевищує визначений критерій, вважаються значними для підприємства, тому заходи і засоби з обробки такого роду ризиків повинні вживатись в першочерговому порядку.

Останнім важливим етапом процесу ризик-менеджменту є здійснення планового перегляду результатів ризик-менеджменту не менше одного разу на рік або, якщо у структурі підприємства або бізнесу вводяться певні видимі зміни, перегляд здійснюється позапланово.

Аналізуючи ризики персональним даним, представлені в Таблиці 1.2 та Таблиці 1.3, можна визначити такі ключові загрози:

а) відмова в обслуговуванні серверів або вихід обладнання з ладу. Загроза цього типу впливає на таку властивість інформації як доступність та, часом, навіть цілісність;

б) ненавмисне пошкодження або знищення даних. Загроза цього типу впливає на всі властивість інформації: цілісність, конфіденційність та доступність;

в) навмисне пошкодження або знищення даних;

г) розголошення даних. Загроза цього типу впливає на таку властивість інформації як конфіденційність;

д) неправильний порядок зберігання даних.

Такий перелік свідчить про значний вплив користувачів системи управління відносинами з клієнтами та питання захищеності даних, що в ній зберігаються та обробляються.

1.8 Огляд існуючих методів захисту даних

Загрози даним у будь-якій інформацій системі існують завжди, навіть як не була б досконало побудована система забезпечення інформаційною безпекою на підприємстві.

Головною задачею, яка стоїть перед компаніями з точки зору інформаційної безпеки є мінімізація ризиків порушення основних властивостей інформації та системи.

Міжнародний стандарт ISO/IEC 27001 «Методи та засоби забезпечення безпеки. Система управління інформаційною безпекою. Вимоги» надає вичерпний перелік рекомендацій щодо підтримки мір управління системою інформаційної

безпеки для забезпечення належного рівня захисту інформації, що зберігається та обробляється в організації.

Відповідно до Додатку А міжнародного стандарту ISO/IEC 27001, по відношенню до процесів забезпечення захисту даних в CRM-системах можна визначити наступну класифікацію організаційних, технічних та фізичних методів захисту інформації:

а) організаційні методи захисту. В рамках цієї категорії стандартом визначаються такі міри захисту:

1) документування політики інформаційної безпеки (А.5.1.1);

2) здійснення аналізу політики інформаційної безпеки (А.5.1.2);

3) розподіл обов'язків по забезпеченню інформаційної безпеки (А.6.1.3);

4) процедури отримання дозволу на використання засобів обробки інформації (А.6.1.4);

5) розгляд питань безпеки при роботі з клієнтами (А.6.2.2);

6) розгляд вимог безпеки в угоді зі сторонніми організаціями, у разі, якщо існує спільна розробка CRM-системи (А.6.2.3);

7) встановлення функцій, обов'язків персоналу по забезпеченню безпеки (А.8.1.1) та умов трудового договору (А.8.1.3) для визначення відповідальності в разі розголошення конфіденційної інформації;

8) відповідальність за нерозголошення даних по закінченню трудового договору (А.8.3.1);

9) анулювання прав доступу до системи після звільнення (А.8.3.3);

10) фіксація та керування змінами (А.10.1.2);

11) розподіл обов'язків (А.10.1.3);

12) розподіл засобів та середовищ розробки, тестування та експлуатації (А.10.1.4);

13) моніторинг послуг, що надаються третіми сторонами (А.10.2.2);

14) управління привілеями користувачів (А.11.2.2);

15) управління паролями користувачів (А.11.2.3);

16) періодичне здійснення перегляду прав доступу користувачів (A.11.2.4);

б) технічні методи захисту. В рамках цієї категорії стандартом визначаються такі міри захисту:

1) захист від шкідливого коду (A.10.4.1);

2) резервування інформації (A.10.2.1);

3) використання засобів контролю мережі (A.10.6.1);

4) забезпечення безпеки мережевих сервісів (A.10.6.2);

5) використання процедур обробки інформації (A.10.7.3);

6) ведення журналів аудиту (A.10.10.1);

7) захист інформації журналів реєстрації подій (A.10.10.3);

8) автентифікація користувачів для здійснення зовнішніх з'єднань (A.11.4.2);

9) контроль мережевих з'єднань (A.11.4.6) та маршрутизації в мережі (A.11.4.7);

10) ідентифікація на автентифікація користувачів (A.11.5.2);

11) завершення сеансів після досягнення певного часу бездіяльності (A.11.5.5);

12) виокремлення систем, що обробляють важливу інформацію, в окремі зони (A.11.6.2);

13) контроль обробки даних в додатках (A.12.2.2);

14) забезпечення цілісності повідомлень (A.12.2.3);

15) застосування криптографічного захисту інформації (A.12.3.1);

16) контроль та обмеження доступу до вихідного коду (A.12.4.3);

17) налаштування сповіщень про події порушення інформаційної безпеки (A.13.1.1);

в) фізичні методи захисту. В рамках цієї категорії стандартом визначаються такі міри захисту:

1) забезпечення контролю доступу до зони зберігання та обробки інформації (A.9.1.2);

2) забезпечення безпеки будівель, приміщень та обладнань (А.9.1.3), а також захисту від зовнішніх загроз та загроз навколишнього середовища (А.9.1.4);

3) забезпечення безпеки дротового зв'язку (А.9.2.3);

4) забезпечення безпеки обладнання, що використовується поза приміщення підприємства (А.9.2.5);

5) захист фізичних носіїв при їх транспортуванні (А.10.8.3);

6) розміщення, захист обладнання (А.9.2.1) та здійснення його належного технічного обслуговування (А.2.4);

7) захист кабельного зв'язку (А.2.3).

Методи забезпечення захисту персональних даних в CRM-системах мало чим відрізняється від загального підходу до здійснення захисту даних в інформаційних системах.

Основною особливістю здійснення захисту даних в системах управління відносинами з клієнтами те, що необхідно приділяти більше уваги діям користувачів та швидко реагувати у разі виникнення помилок та інших інцидентів, пов'язаних з модифікацією або видаленням даних клієнтів.

Висновки за розділом 1

В даному розділі було визначено критичність такого активу підприємств як персональні дані клієнтів та співробітників та здійснено аналіз нормативно-правової бази, яка регулює питання захисту персональних даних.

Було визначено основні функції сучасних систем управління відносинами з клієнтами.

Відповідно до проведеного ризик-менеджменту, який було здійснено за методологією IT-Grundshutz з використанням IT-Grundshutz Catalogues та моделі CIA, визначено основні загрози персональним даним, що зберігаються та обробляються в системах управління відносинами з клієнтами, а саме:

– неприпустимі дії співробітників;

- втрата даних клієнтів;
- атаки на роботу системи;
- низька якість ПО;
- шахрайство з електронними документами;
- крадіжка конфіденційної інформації.

В розділі було виконано аналіз статистики здійснення інцидентів інформаційної безпеки з особливим акцентом на питання витоку даних. Відповідно до цього аналізу було визначено, що ключовою загрозою персональним даним у системах управління відносинами з клієнтами є великий вплив людського фактору, а основним ризиком – ризик помилкового введення даних або умисного їх пошкодження чи видалення.

РОЗДІЛ 2
ОГЛЯД МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СУЧАСНИХ СИСТЕМАХ УПРАВЛІННЯ ВІДНОСИНАМИ З КЛІЄНТАМИ

2.1 Архітектура сучасних систем управління відносинами з клієнтами

Захист даних у CRM-системі так чи інакше залежить від того, як ця система побудована, які компоненти має та як вони взаємодіють один з одним.

Організація інформаційної системи, втілена в її компонентах, їх взаємозв'язках між собою та з оточенням представляє собою архітектуру системи. Більшість сучасних систем управління відносинами з клієнтами будується на багаторівневій (або як ще кажуть «монолітній») та мікросервісній архітектурі, проте існують і інші архітектурні шаблони, які регулюють взаємодію компонентів системи.

У даній роботі буде розглянуто багаторівневу (монолітну) та мікросервісну архітектуру – шаблони, які частіше за все зустрічаються у сучасних CRM-системах.

Так чи інакше, всі компоненти системи, не залежно від того, як вона побудована, з однієї сторони, виконують окремі один від одного функції, а з іншої взаємодіють один з одним. Відповідно до цього захист даних необхідно здійснювати окремо на кожному з логічних рівнів системи та забезпечувати захищену передачу даних від одного компоненту до іншого.

Ще однією особливістю у питанні захисту даних CRM-систем є те, що вона в будь-якому випадку передбачає взаємодію з кінцевим користувачем. Автоматизовані системи, в яких обробка даних здійснюється майже без допомоги людини, можуть нехтувати такими засобами захисту як повторна перевірка дії видалення даних, застосування правил та валідацій під час введення інформації до системи і тому подібне. В CRM-системах це ні в якому разі не можна упускати, адже, як вже було сказано раніше, користувач – ключовий елемент системи управління відносинами з клієнтами.

2.1.1 Багаторівнева архітектура

Традиційним архітектурним шаблоном для Enterprise-додатків є багаторівнева архітектура, яка організовується шляхом розподілу додатку на рівні, які виконують певні логічні функції.

Частіше за все зустрічаються використання трирівневої архітектури, що передбачає наявність таких компонентів програми:

– клієнтську програму (зазвичай говорять «тонкий клієнт» або термінал);
– сервер додатків;
– сервер бази даних.

Клієнт являє собою інтерфейсний компонент, який представляє собою перший рівень взаємодії з кінцевим користувачем, тобто додаток з яким безпосередньою працює користувач.

Загальні вимоги, які висуваються до цього рівня архітектури такі:

– він не повинен мати прямих зв’язків з базою даних (задля забезпечення вимог безпеки);
– він не повинен бути навантаженим основною бізнес-логікою (за вимогами масштабованості та для уникнення помилок по типу відмов в обслуговуванні, що впливають на доступність системи та інформації, що в ній зберігається та обробляється);
– він не повинен зберігати стан додатку (за вимогами надійності системи, задля уникнення загроз аналогічно попередньому пункту).

Зазвичай, на перший рівень архітектури виноситься достатньо проста бізнес-логіка як, наприклад, перевірка значень, що вводяться, на відповідність формату або іншу валідацію; такі операції з даними як групування, підрахунок суми значень тощо.

Отже на інтерфейсний компонент багаторівневої архітектури виносяться ті розрахунки та перевірки, які не потребують значних обчислень чи використання складних алгоритмів.

Другий рівень являє собою сервер додатку, тож на цьому рівні виконується більша частина бізнес-логіки за винятком лише тієї частини, яка винесена в збережені процедури та тригери на рівні баз даних. Сервер додатків також часто називають «шаром логіки» саме через те, що він по суті являється зв'язуючим компонентом, який координує систему та обробляє дані для відображення їх кінцевому користувачу.

Сервер баз даних, власне, забезпечує зберігання даних та представлений як третій рівень багаторівневої архітектури.

Приклад простої багаторівневої архітектури зображено на рис. 2.1.

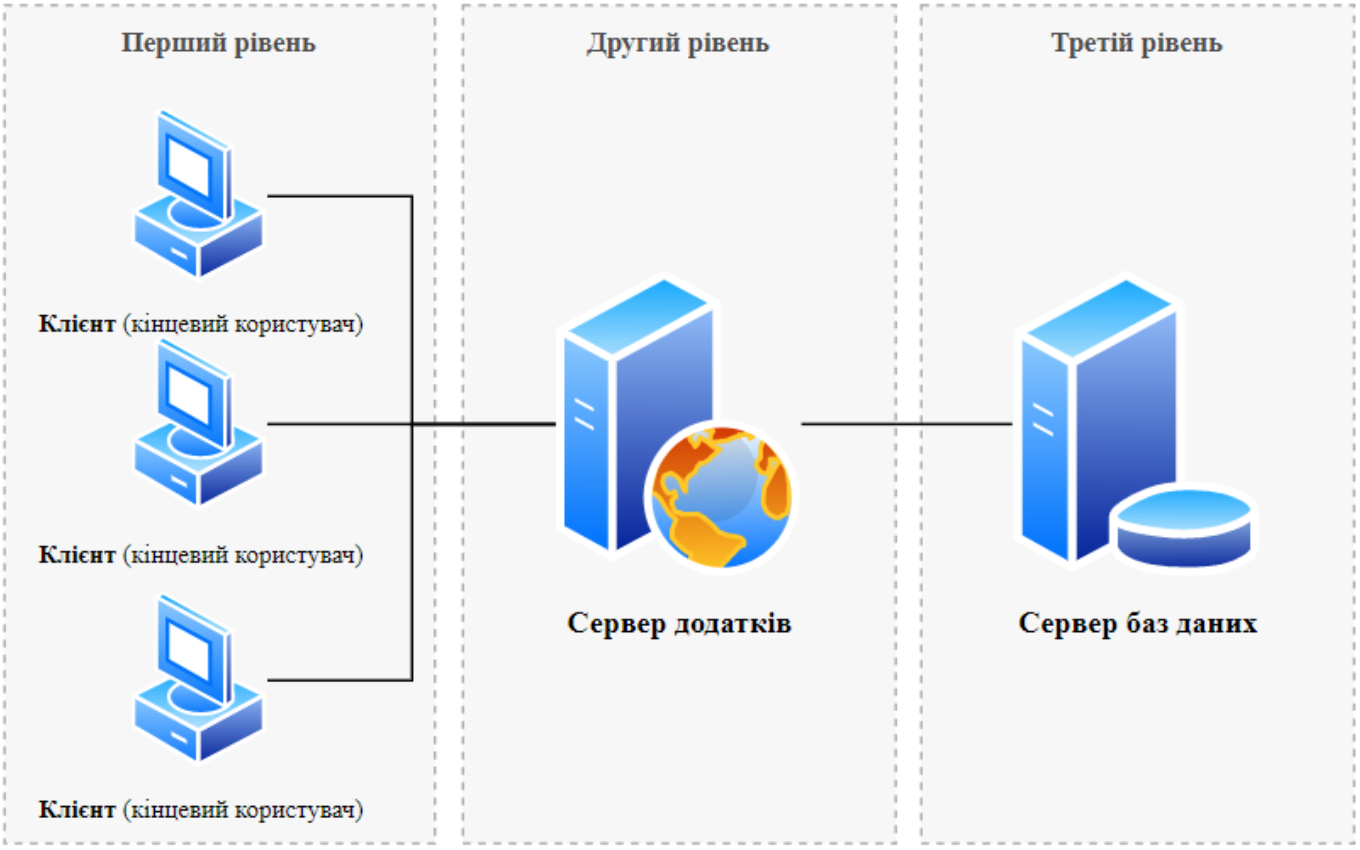

Рисунок 2.1 – Схема багаторівневої архітектури

Як можна побачити, представлена на рис. 1.2 схема немає виходу до мережі Інтернет. Враховуючи відсутність виходу до глобальної мережі будемо вважати, що в даній системі працює невелика кількість користувачів та локальна мережа забезпечується під'єднанням усіх компонентів системи один до одного без використання бездротового каналу передачі інформації. В такому випадку захист

інформації, що обробляється у системі, та захист основних компонентів системи здійснюється безпосередньо на робочих станціях та полягає у фізичному захисті апаратних засобів, кабелів, робочих місць користувачів.

Звичайно у сучасних умовах майже всі інформаційні системи мають вихід до глобальної мережі Інтернет та бездротові канали передачі даних, а більшість систем має відносно велику кількість користувачів.

Зважаючи на все вищесказане, схема сучасної багаторівневої архітектури повинна налічувати компоненти безпеки, які можуть бути використані для зменшення ризику порушення цілісності та конфіденційності даних, а також балансувальники навантажень, які попереджують ризик порушення доступності системи та даних у разі ймовірної відмови одного або декількох компонентів системи (наприклад у разі здійснення на систему DoS або DDoS атаки).

Захищена інформаційна система, побудована за принципами багаторівневої архітектури буде виглядати наступним чином (рис. 2.2):

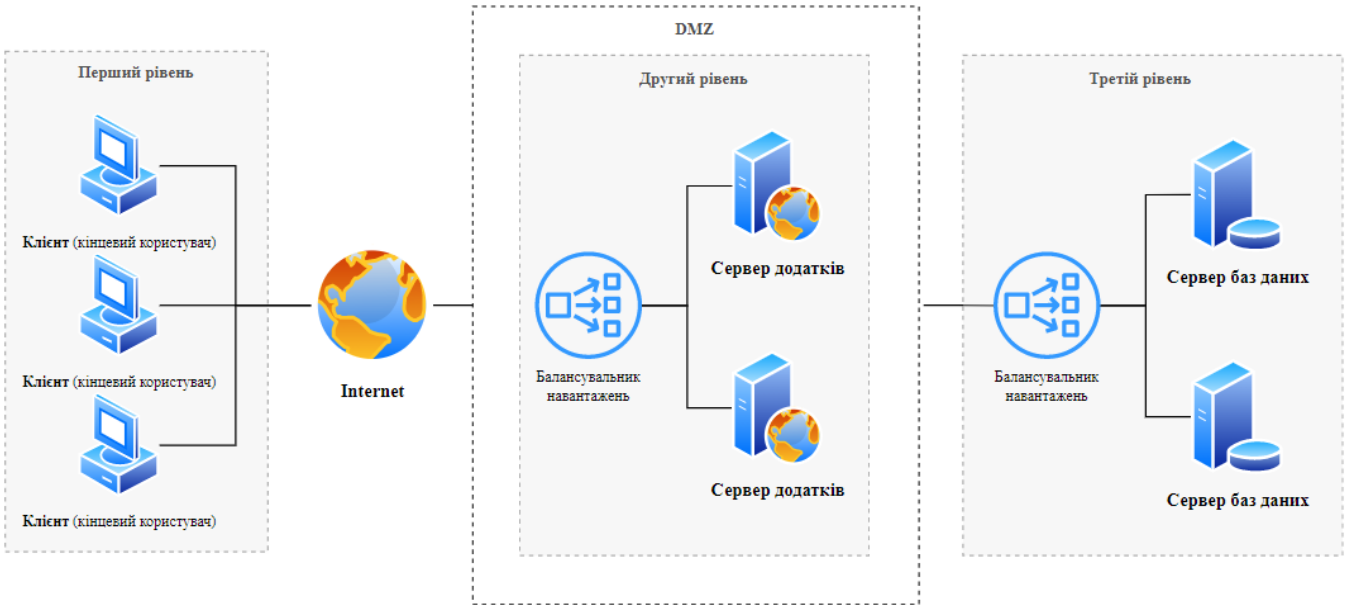

Рисунок 2.2 – Схема захищеної багаторівневої інформаційної системи

В захищеній системі виділена підмережа – демілітаризована зона (далі – DMZ), яка забезпечує додатковий рівень захисту конфіденційних даних, що знаходяться у внутрішній мережі, використовуючи брандмауери для фільтрації трафіку, що надходить із-зовні та з локальної мережі.

Окрему увагу слід приділити такому елементу системи як балансувальник навантаження. Даний елемент інформаційної системи може бути як програмним, так і апаратним та використовується для роботи системи у відмовостійкому режимі. Часто також можна зустріти використання балансувальнику HTTP / HTTPS-трафіку з підтримкою протоколу WebSocket – HAProxy.

Балансувальник HAProxy підримує такі операційні системи як:

– Linux;
– FreeBSD;
– OpenBSD;
– Solaris;
– AIX.

Крім цього, балансувальник HAProxy являється програмою з відкритим кодом, що дозволяє переконатися у відсутності вразливостей додатку [16].

Для більшої надійності системи рекомендується використовувати балансувальник навантаження працює в режимі Active / Stand-by, тобто один з балансувальників знаходиться в активному режимі, інший – в режимі очікування; у разі виникнення проблем в активній системі, її роботу заміняє резервна система, поки проблема не буде вирішена.

Отже, до переваг багаторівневої архітектури можна віднести наступне:

– простота конфігурації системи: кожен рівень такої архітектури виконує чітко обмежений набір функцій, тому здійсненння налаштування окремого рівня або внесення змін до їх конфігурації з меншою ймовірністю призведе до виникнення конфліктів між рівнями. Така перевага дозволяє компаніям, в яких розробка програмного забезпечення ведеться кількома командами, кожна з яких відповідає за окремий рівень додатку, розподілити свої компетенції для реалізації функцій різних рівнів додатку;

– масштабованість додатку, що являється важливим аспектом інформаційних систем та полягає у можливості збільшувати продуктивність, збільшуючи програмно-апаратні ресурси системи. Прикладом горизонтального

масштабування є використання балансувальників навантажень, зображених на схемі рис. 2.2, або об’єднання серверів у кластери;

– високий рівень надійності: розмежування функцій системи на окремі рівні забезпечує мінімізацію негативного впливу одного компоненту на інші;

– високий рівень безпеки: сервер додатку багаторівневої архітектури діє в якості центральної точки, використання якої дозволяє постачальникам сервісів здійснювати керування доступу до даних. Такий підхід дозволяє змістити відповідальність за автентифікацію з потенціально небезпечного рівня клієнта на рівень серверу додатків, додатково захищаючи рівень баз даних;

– низькі вимоги до апаратного забезпечення кінцевих користувачів: як вже було зазначено, більша частина бізнес логіки виконується на рівні серверу додатків або, за умови використання збережених процедур та тригерів, переноситься на рівень баз даних. За таких умов навантаження на термінали клієнтського рівня мінімальні та не потребують значних витрат на апаратне забезпечення.

Проте, існує також ряд недоліків багаторівневої архітектури, таких як:

– високі вимоги до продуктивності серверів додатків та баз даних. Пояснюється це, звичайно, тим, що виконання складних алгоритмів потребує великих потужностей системи. Крім цього, обробка даних зазвичай передбачає створення нових записів у таблицях баз даних, саме тому сервер баз даних повинен мати достатньо місця на диску задля уникнення ситуацій, коли робота кінцевого користувача блокується через недолік місця у базі даних;

– складність адміністрування та усунення помилок. Розподіл компонентів системи на логічні рівні передбачає, що під час обробки інформація проходить всі рівні: змінена в інтерфейсі системи інформація проходить через шар бізнес-логіки до серверу баз даних, після чого здійснюється її збереження у системі. У разі, якщо на якомусь з етапів дані були модифіковані або втрачені, на дослідження такого інциденту буде витрачено немало часу, оскільки необхідно буде здійснювати відстеження даних на всіх рівнях системи;

– певна залежність рівнів один від одного, тому при виникненні збоїв, наприклад, на рівні баз даних, клієнт та сервер додатків не зможе виконувати виконувати свої функції, а отже весь додаток стане недієздатним.

Нерідко в цілях економії або через недостатність апаратних ресурсів сервер додатків та сервер баз даних розміщують на одному персональному комп'ютері, що, по-перше, збільшує ризик порушення конфіденційності, цілісності та доступності одразу двох компонентів системи та, по-друге, з великою ймовірністю призводить до зниження продуктивності системи.

2.1.2 Мікросервісна архітектура

Сучасні підприємства, у CRM-системах яких виконується багато різної бізнес-логіки, все частіше при розробці CRM-системи намагаються використовувати архітектурний шаблон, що має назву «мікросервіси».

Головною відмінністю цього шаблону від багаторівневої архітектури є те, що єдиний додаток складається з набору незалежних один від одного сервісів, кожен з яких самостійно може виконувати певну бізнес-логіку.

Складові багаторівневої архітектури поділені на функціональні рівні – користувацький інтерфейс, бізнес-логіка та база даних, при цьому кожен з рівнів не може функціонувати окремо один від одного. Додаток, побудований на мікросервісах, передбачає поділ системи на логічні рівні, тож кожен з сервісів базується на бізнес-вимогах, є повністю автономним та може функціонувати самостійно.

Основними та головними особливостями мікросервісної архітектури є:

– простота сумісної розробки: великі підприємства можуть розділювати реалізацію сервісів по окремим командам, що значно прискорює час створення нових додатків. Це забезпечується також тим, що сервіси можуть бути написані на різних мовах програмування та використовувати різні технології зберігання даних;

– більш надійність у порівнянні з багаторівневою архітектурою: відмова одного з компонентів системи не передбачає відмову всієї системи, оскільки всі вони являють собою окрему структуру та не залежать один від одного;

– легкість внесення нових додаткових функцій до системи: достатньо розробити та під'єднати до основної системи один мікросервіс замість того, щоб вносити зміни моноліт.

Схема типової мікросервісної архітектури представлена на рис. 2.3.

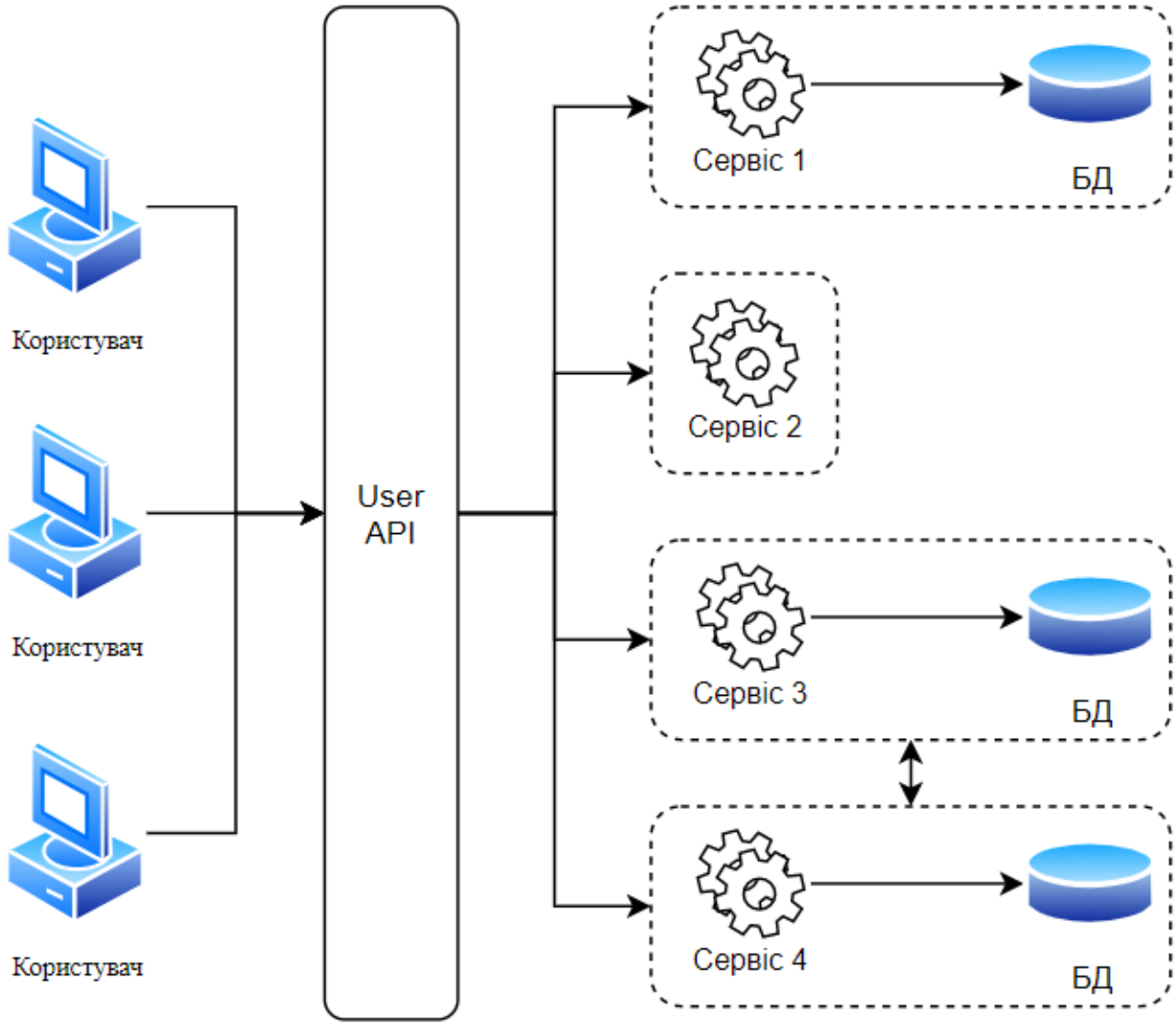

Рисунок 2.3 – Типова схема мікросервісної архітектури

Як можна побачити, часом мікросервіси навіть не мають бази даних та виконують лише якусь бізнес-логіку; деякі сервіси працюють повністю окремо один від одного, а деякі взаємодіють під час обробки даних.

Така автономність сервісів спричинює також ряд недоліків мікросервісної архітектури:

– складність розробки розподілених систем. Вона викликана тим, що не дивлячись на незалежність сервісів, у разі, коли виникає необхідність здійснення взаємодії двох або більше сервісів всередині системи, можуть виникати певні складнощі обробки запитів, що обробляються між ними;

– складність керування базою даних. На відміну від монолітної архітектури кожен мікросервіс може мати свою окрему базу даних, тож фінансові та людські ресурси на її адміністрування та забезпечення належного захисту інформації, що в ній зберігається, зростають прямопропорційно кількості цих баз даних;

– актуальність даних в окремій базі даних. Оскільки окремі мікросервіси мають власні сховища даних, інформація щодо змін цих даних не розповсюджується системою миттєво, тож можуть виникати ситуації за яких певні мікросервіси деяких проміжок часу матимуть застарілі дані.

Зважаючи на те, що основною функцією CRM-систем є зберігання та систематизація персональних даних клієнтів, саме база даних відіграє роль найважливішого компонента системи.

Тому ідеологічною моделлю функціонування CRM-систем частіше за все є багаторівнева архітектура, що включає централізоване сховище даних, яке обслуговує весь процес взаємодії в клієнтами.

2.2 Огляд методів захисту даних в CRM-системах на прикладі системи Creatio

Великий попит систем управління відносинами з клієнтами формує створення великої кількості рішень на ринку інформаційних технологій. Для вибору системи, підприємства звертають увагу на зручність інтерфейсу, можливість розширення функцій системи та, насправді, рідко коли беруть до уваги методи захисту, які вона надає.

В даній роботі для здійснення практичного аналізу методів захисту персональних даних у сучасних системах було обрано CRM-систему Creatio.

Лінійка продуктів системи Creatio представляє собою єдину хмарну CRM-систему для великих та середніх компаній, що дозволяє об'єднувати та прискорювати процеси продажів, маркетингу та сервісу, а також внутрішні операційні процеси підприємств. Дана система є не лише системою управління взаємовідносинами з клієнтами, а ще й платформою, яка містить функціонал управління бізнес процесами (англ. Business Process Management, BPM).

Основними продуктами, розробленими компанією Terrasoft, є:

– Sales Creatio;
– Marketing Creatio;
– Service Creatio;
– Studio Creatio.

Ці продукти розробдені для управління продажами, маркетингом та сервісом відповідно. Крім цього існує онлайн-каталог Marketplace, на якому клієнтам доступні десятки готових рішень, що дозволяють кастомізувати рішення платформи відповідно до потреб підприємства.

Загалом, базові можливості CRM-системи Creatio дозволяють збирати всю інформацію про клієнтів та контрагентів в єдиній системі, актуалізувати її з відкритих джерел, за допомогою інтеграцій зі сторонніми системами; гнучко налаштовувати весь цикл продажів та створювати каталог всіх продуктів чи сервісів з повним набором їх характеристик та особливостей; використовувати єдине вікно операторів контакт-центру, яке дозволяє користувачам виконувати всі свої робочі функції, не переключаючись між розділами системи [17].

Базова схема архітектури основного додатку Creatio, представлена на рис. 2.4, не дуже відрізняється від типової схеми монолітної архітектури (рис. 2.1).

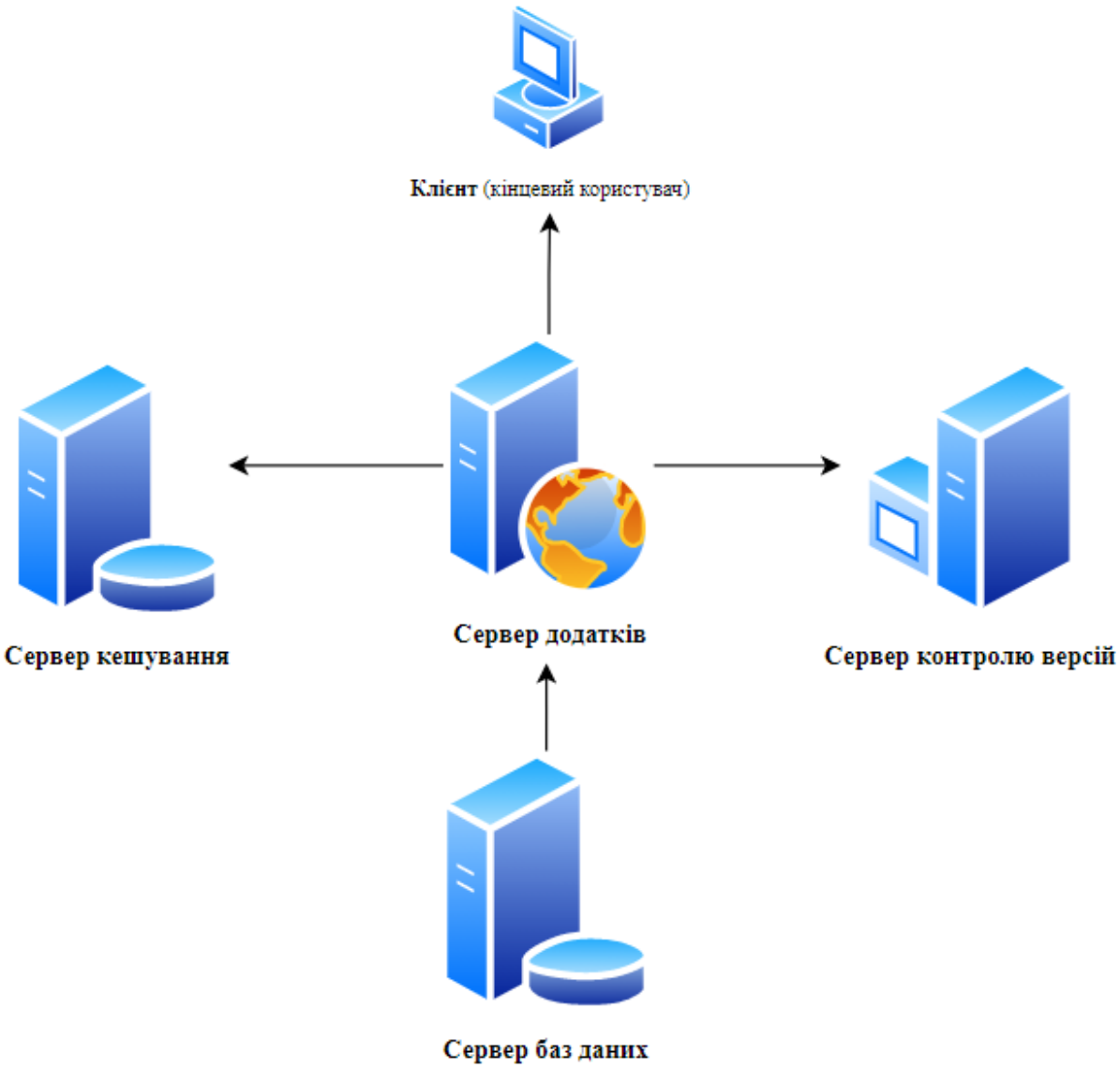

Рис. 2.4 – Схема архітектури основного додатку Creatio

У порівнянні зі стандартною схемою багаторівневої архітектури, схема архітектури основного додатку Creatio включає в себе також сервер кешування даних та сервер контролю версій (SVN, англ. Subversion), який є опціональним компонентом схеми та використовується лише у випадку існування користувацької розробки функціоналу системи.

Слід зазначити, що така типова схема може бути використана на підприємствах з невеликою кількістю користувачів (близько 20 – 100) та не потребує значних витрат на потужні сервери – достатньо використання лише трьох обов'язкових виділених серверів: серверу додатків, серверу баз даних та серверу кешування.

Користувачами CRM-систем як мінімум є менеджери по роботі з клієнтами, які складають зазвичай більшу частину співробітників підприємств. Крім того, сучасні системи дозволяють налагоджувати на автоматизовувати процеси за участю декількох функціональних ролей, тому часом кількість користувачів CRM-системи може налічувати понад 500 співробітників.

Використання багаторівневої архітектури передбачає невисоке навантаження на робочі місця кінцевих користувачів, що мінімізує витрати власників підприємств на забезпечення всіх співробітників потужними персональними комп'ютерами та іншим обладнанням.

Розглянемо більш детально кожен окремий компонент CRM-системи та засоби забезпечення захисту, які застосовуються на кожному рівні.

2.2.1 Забезпечення захисту на рівні серверу додатків

Відповідно до структури багаторівневої архітектури, сервер додатків виконує основну обчислювальну роботу системи. Додаток CRM-системи Creatio працює на платформі .NET Framework під управлінням Internet Information Services (IIS) та складається з:

- завантажувача (WebAppLoader);
- конфігураційної частини (WebApp).

Internet Information Services (IIS) – інтегрований в серверні операційні системи Windows модуль, що дозволяє без особливих труднощів встановити і налаштувати веб-додаток як для власних потреб в рамках локальної мережі, так і для загального використання в мережі Internet [18].

Сучасні CRM-системи потребують організації централізованої обробки та зберігання даних, оскільки вони не обмежуються настільним програмним забезпеченням, яке встановлюється на персональні комп'ютери користувачів. Частіше за все в якості клієнтського ПЗ використовуються браузер, що значно полегшує процеси оновлення застосунку.

IIS сервер (він же сервер додатків) забезпечує прийом HTTP запитів, що надсилаються віддаленими робочими станціями та виконує функцію провідника даних по таким процесам їх обробки:

– автентифікація;
– авторизація;
– журналювання подій тощо.

Кожен з користувацьких запитів супроводжується так само HTTP відповіддю IIS сервера. Основне призначення IIS сервера CRM-системи Creatio – виконання службових функцій системи, і подальше перенаправлення користувачів в основну програму Creatio.

Доступ користувачів до конфігураційної частини, яка відповідає за роботу бізнес-логіки системи, здійснюється після обробки запиту на автентифікацію. Автентифікація в IIS сервері здійснюється в два етапи:

– перший: на рівні серверу, спільний для всіх додатків;
– другий: на рівні окремого веб-додатку.

Базовими механізмами автентифікації IIS сервера, які частіше за все використовуються в CRM-системи Creatio є:

а) анонімна автентифікація: механізм, який не потребує від користувача вводу логіку та паролю і забезпечує доступ до веб-додатку шляхом управління доступу до директорій та файлів локального облікового запису IIS_IUSR (рис. 2.5);

б) базова автентифікація: механізм, за якого здійснюється перевірка введеного користувачем логіну та паролю. Даний протокол автентифікації передбачає відкриту передачу даних, тож зловмисники можуть перехопити цю інформацію, використовуючи різноманітні аналізатори трафіку. Зважаючи на це, використовувати базову автентифікацію в CRM-системах не рекомендується;

в) Windows автентифікація: механізм, який дозволяє використовувати доменну авторизацію для отримання доступу до веб-додатку, та взаємодіє зі службою каталогів Active Directory, що дозволяє адміністратору безпеки налаштовувати групові політики доступу до директорій та файлів (рис. 2.6).

Для реалізації Windows автентифікації використовуються протоколи:

1) NTLM;
2) Negotiate (протокол Kerberos) [18].

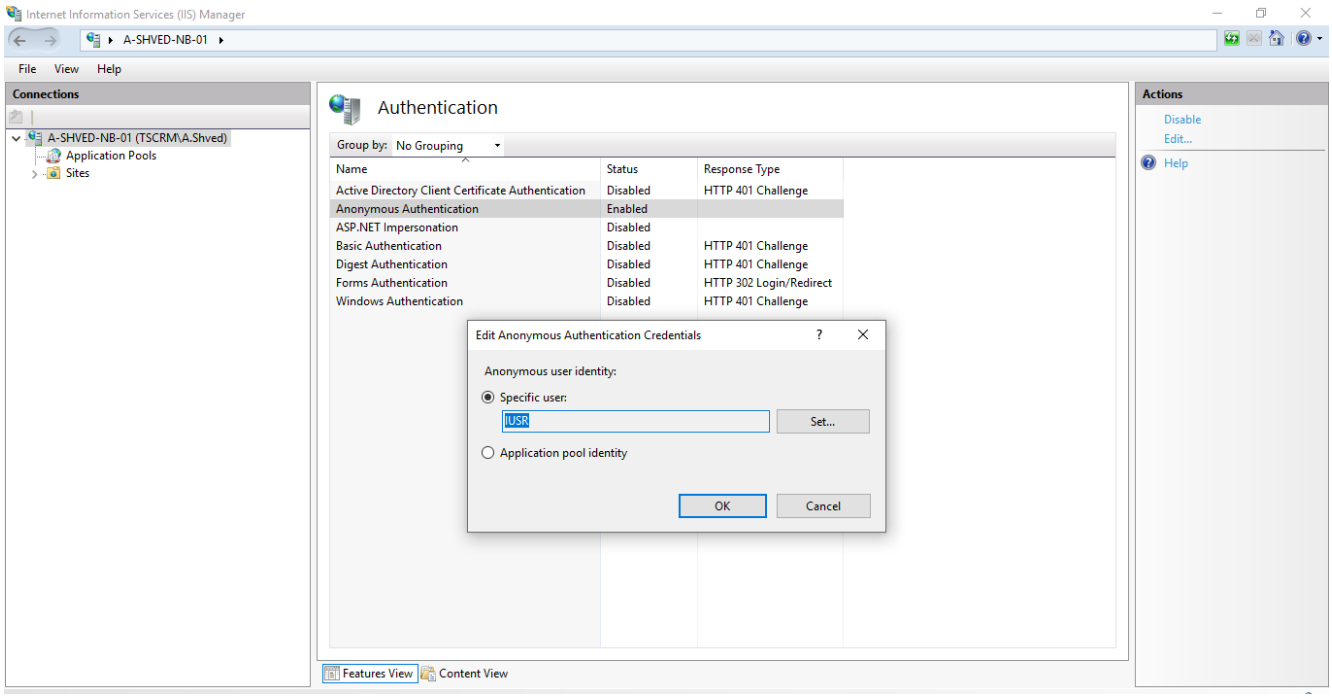

Рисунок 2.5 – Установка протоколів анонімної автентифікації IIS сервера

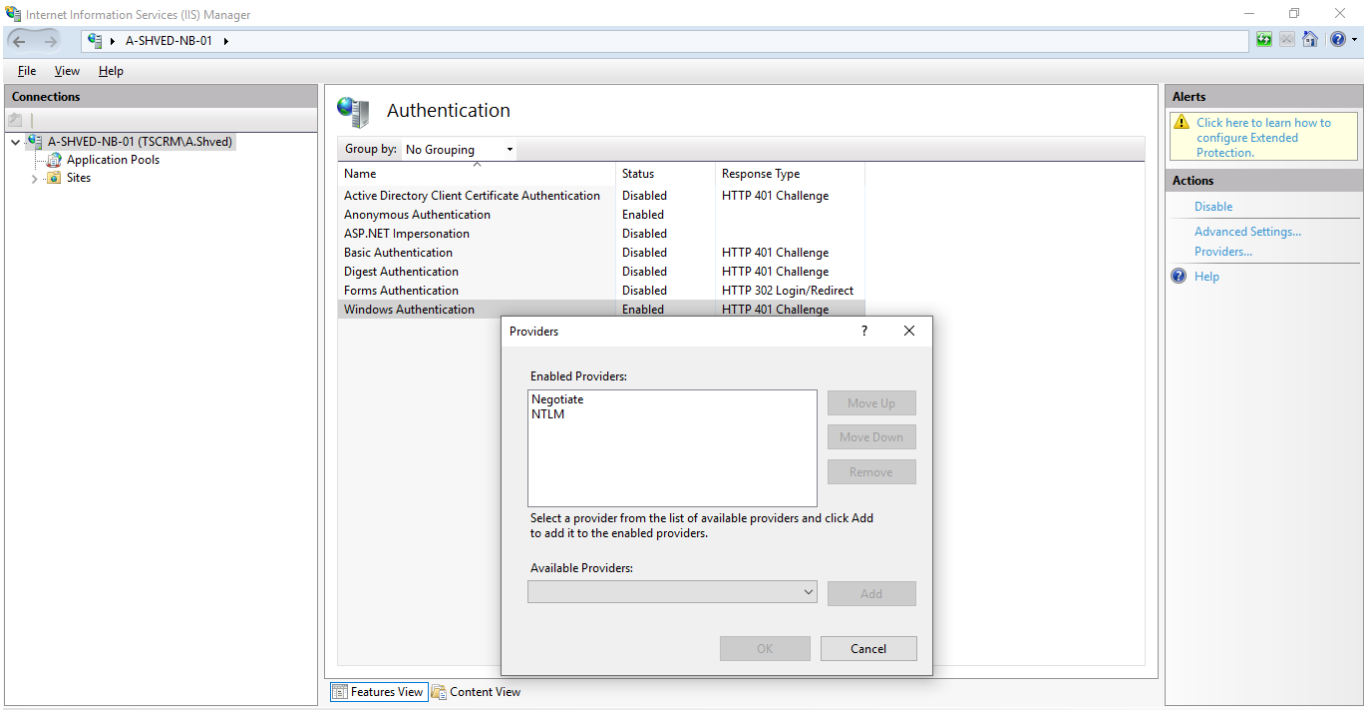

Рисунок 2.6 – Установка протоколів Windows автентифікації IIS сервера

2.2.2 Забезпечення захисту на рівні серверу баз даних та серверу Redis

В базі даних додатку зберігаються користувацькі дані, дані, необхідні для роботи системи та конфігураційні налаштування. Найбільш використовуваними системами управління баз даних Creatio є:

- MS SQL Server,
- Oracle,
- PostgreSQL [20].

Дієвим способом захисту даних на рівні серверу додатків є інтеграція CRM-систем з системами безпеки системи управління бази даних (СУБД).

В сучасних СУБД використовуються гібридні моделі захисту, які включають наступні моделі безпеки:

- дискреційна;
- мандатна;
- рольова.

З усіх моделей безпеки найзручнішою для користувачів є рольова модель, оскільки за її допомогою можна створювати багаторівневі системи захисту [20].

З усіх схем автентифікації найчастіше використовується парольний захист, зважаючи на його дешевизну та простоту. В CRM-системі Creatio паролі користувачів шифруються 128-бітним ключем та зберігаються у базі даних в нечитабельному вигляді, що мінімізує ймовірність викрадення викрадання логіну та паролю користувач.

Сервер кешування Redis відповідає за зберігання даних користувача і додатку (профіль користувача, сесійні дані тощо), зберігання кешованих даних, обмін даними між вузлами веб-ферми.

Redis підтримує такі стратегії зберігання даних:

- зберігання даних лише в пам'яті;
- періодичне збереження даних на диск (за замовчуванням);
- лог транзакцій;
- реплікація [17].

В Creatio зберігання даних здійснюється в пам’яті з періодичним збереженням резервної копії на диск.

Як вже було зазначено раніше, великим підприємствам недостатньо базової функціональності системи Creatio, тому компанії намагаються власними силами або через посередників розширювати функціонал системи.

Сервер системи контролю версій – є опціональним та використовується саме у тому випадку, коли паралельно з експлуатацією системи необхідно на платформі організувати розробку користувальницької конфігурації.

Отже схематично рівні захисту даних, що зберігаються та обробляються у CRM-системі Creatio, можна зобразити наступним чином (рис. 2.7):

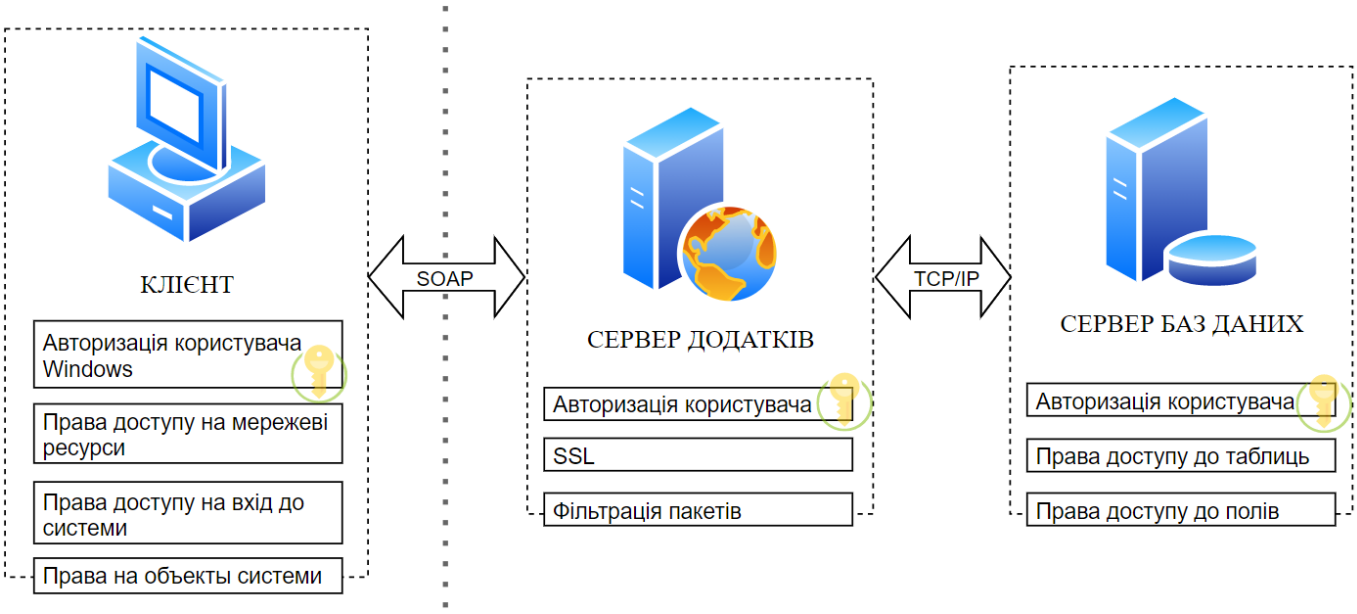

Рисунок 2.7 – Схематичне зображення рівнів захисту CRM-системи Creatio

Відповідно до того, які завдання ставить підприємство перед CRM-системою, зростають і її масштаби та необхідність здійснення інтеграцій з сторонніми системами та сервісами. CRM-система Creatio дозволяє інтегруватись с веб-сервісами, які в свою чергу підтримують підключення з використанням SSL протоколу, що дозволяє використовувати шифрування з відкритим ключем для автентифікації і шифрування клієнт-серверних з'єднань. [17]

Для CRM-системи організації, що складається з великих бізнес-процесів, які виконують складні, ресурсномісткі функції, та кількість користувачів якої сягає

понад 100, 200 або навіть 1000 користувачів, використання одного серверу додатків, одного серверу баз даних та серверу кешування вже не буде достатнім для забезпечення безперервної та стабільної роботи системи.

В такому випадку, підвищити продуктивність великих проектів дозволяє горизонтальне масштабування системи. При цьому в схему архітектури системи Creatio (рис. 2.8) додаються наступні компоненти:

– балансувальник навантажень;
– резервний балансувальник навантажень;
– ревервний сервер кушевання Redis.

Крім цього, замість одного серверу додатків використовують декілька серверів, об’єднаних у так звану Web-ферму, та декілька серверів баз даних, об’єднаних у кластер баз даних.

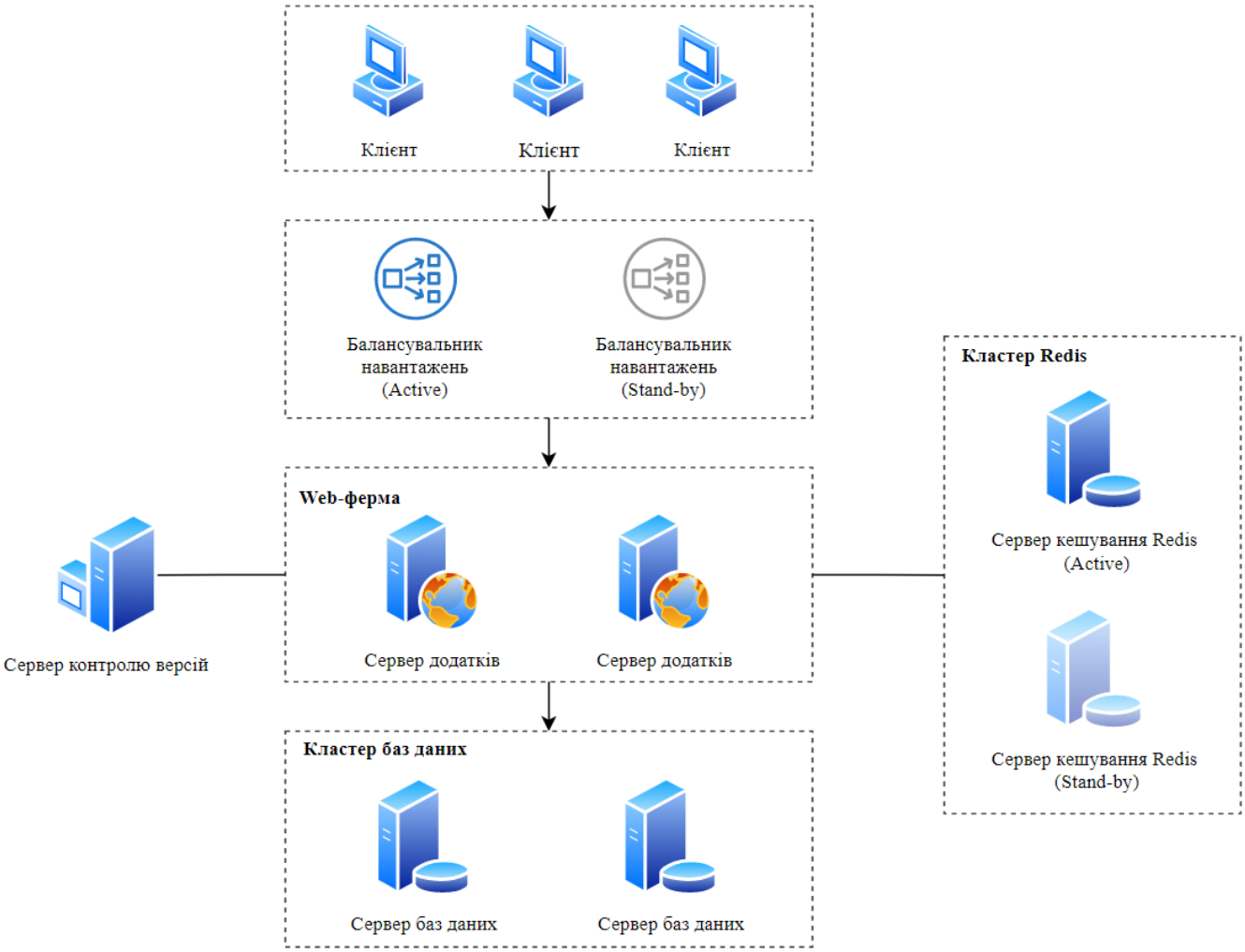

Рис. 2.8 – Схема горизонтального масштабування архітектури основного додатку Creatio

2.2.3 Забезпечення захисту на робочих місцях кінцевих користувачів

Ще одним важливим компонентом системи, якому слід приділити уваги, є робочі станції кінцевих користувачів. Системою Creatio передбачений метод захисту, який мінімізують ризики здійснення атак на систему способом Brute-Force, тобто здійснення атаки «грубої сили» для підбору паролю користувача.

Власники систем самостійно можуть обрати для себе ту кількість спроб вводу логіну та паролю до системи, яка буде вважатись підозрілою. Для цього в системі існує системне налаштування «Кількість спроб входу, здійснених до попереджувального повідомлення», в якому системний адміністратор може встановити значення за замовчуванням, після перевищення якого користувачу виводиться повідомлення з попереджувальним текстом (рис. 2.9).

Час, на який блокується доступ до системи, також визначається відповідним системним налаштуванням.

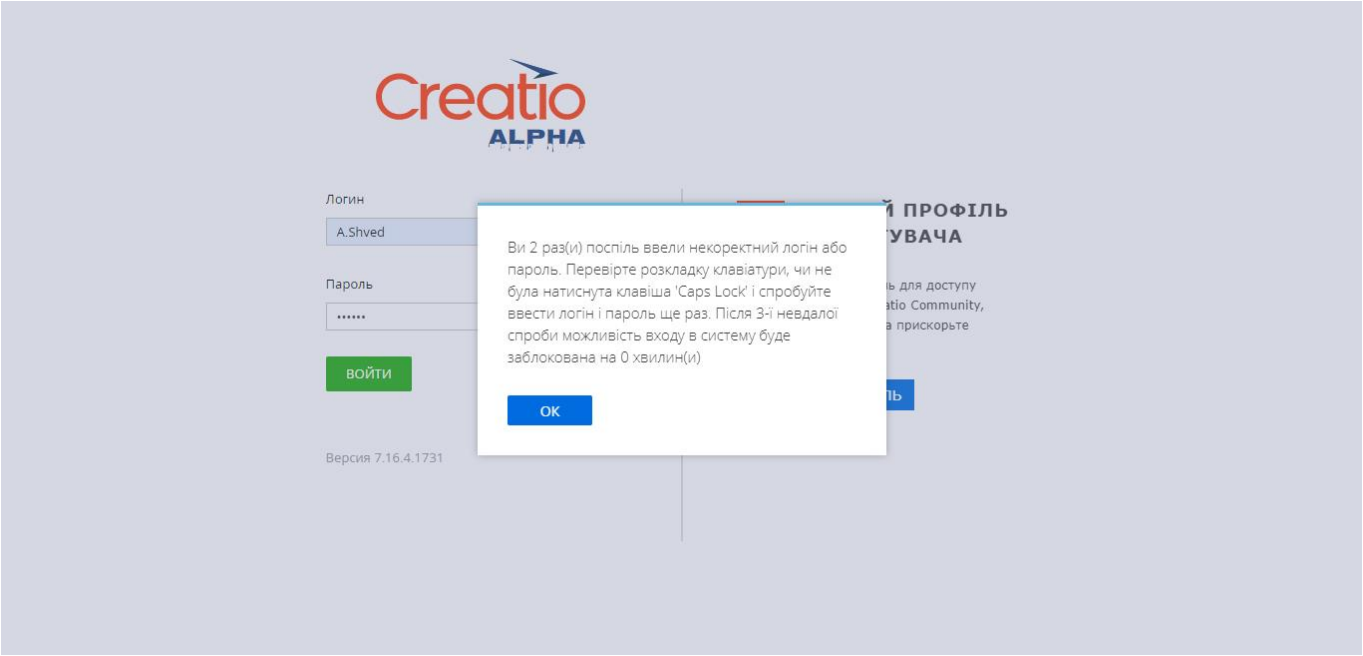

Рисунок 2.9 – Інтерфейс системи Creatio при здійснені підбору паролю

Загальна кількість спроб входу також визначається системним адміністратором в системному налаштуванні під назвою «Кількість спроб входу». Якщо кількість спроб перевищує значення, встановленого в налаштуванні (в даному

прикладі 3), обліковий запис користувача деактивується (рис. 2.10) і може бути активований лише системним адміністратором.

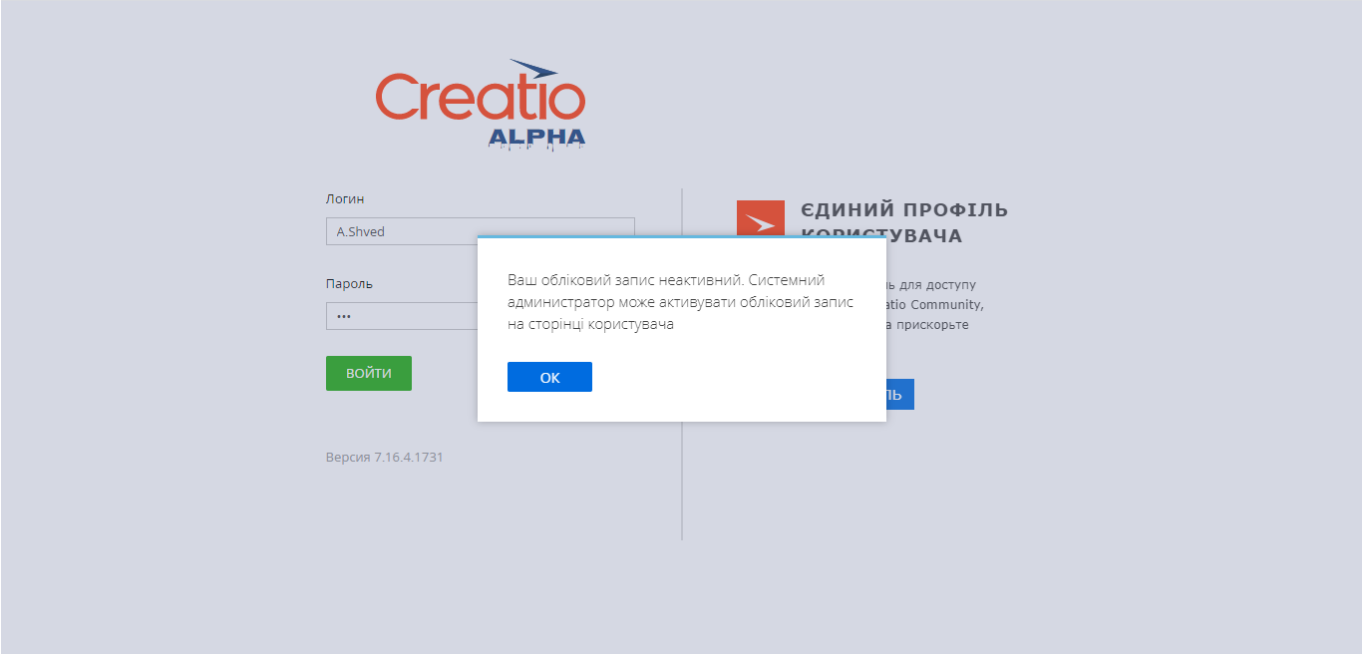

Рисунок 2.10 – Повідомлення про деактивацію облікового запису в інтерфейсі системи Creatio.

Частковий перелік системних налаштувань, що відносяться до питань захисту даних та встановлення яких передбачає система Creatio, наведено у Таблиці 2.1. Відповідність забезпечення вимог безпеки встановлюється відповідно до міжнародного стандарту ISO/IEC 27001 «Методи та засоби забезпечення безпеки. Система управління інформаційною безпекою. Вимоги». Додаток А [23].

Таблиця 2.1

Перелік системних налаштувань безпеки даних CRM-системи Creatio

Налаштування	**Опис**	**Контролі безпеки**
Список дозволених розширень файлів	Містить перелік файлів, які можна завантажувати у систему. Мінімізує ймовірність порушення системних файлів.	**A.12.4** Безпека системних файлів

продовження табл. 2.1

Налаштування	Опис	Контролі безпеки
Дозволити роботу з невідомими типами файлів	Ввімкнення налаштування передбачає, що система буде працювати з файлами, типи яких вона не змогла визначити. Рекомендується не вмикати це налаштування.	
Кількість спроб входу	Мінімізує ймовірність підбору паролю користувачів.	**A.11.2** Управління доступом користувачів
Термін дії паролю, днів	Мінімізує ймовірність викрадення паролю або його підбору.	
Кількість паролів, які аналізуються	Визначає кількість попередніх (останніх) паролів користувачів, з якими порівнюється новостворюваний пароль. Не рекомендується встановлювати значення 0, щоб гарантувати зміну паролю користувачем, а не повторення попереднього. Мінімізує ймовірність викрадення паролю або його підбору.	

продовження табл. 2.1

Налаштування	Опис	Контролі безпеки
Складність паролю: Мінімальна довжина	Налаштування, які встановлюють складність паролю користувача. Рекомендується застосовувати в паролі: хоча б один символ верхнього регістру, один символ нижнього регістру, один спеціальний символ, довжина паролю мінімум 6-8 символів. Мінімізує ймовірність підбору паролю.	
Складність паролю: Мінімальна кількість символів нижнього / верхнього регістру		
Складність паролю: Мінімальна кількість цифр		
Складність паролю: Мінімальна кількість спеціальних символів		
Таймаут сеансу користувача, хв.	Налаштування, яке дозволяє визначити таймаут сеансу кожного окремого користувача у системі.	**A.11.5.5** Періоди бездіяльності в сеансах зв'язку
Діапазон дозволених IP-адрес	Налаштування дозволяє встановити перелік IP-адрес, з яких кожен окремий користувач може отримати доступ до системи.	**A.11.4.6** Контроль мережевих з'єднань

продовження табл. 2.1

Налаштування	Опис	Контролі безпеки
Реєструвати події управляння сесіями користувачів	Налаштування дозволяє ввімкнути реєстр подій управління сесіями користувачів, а також фіксувати початок та завершення сеансу користувача та IP-адресу, з якої користувачем було здійснено вхід до системи.	**A.10.10** Моніторинг **A.11.4.3** Ідентифікація обладнання у мережі

Крім всього вищезазначеного, CRM-система Creatio дозволяє налаштувати реєстрацію подій зміни цих значень, реєстрацію змін структури організаційних та функціональних ролей системи, реєстрацію факту авторизації користувачів.

Проаналізувавши на прикладі системи Creatio методи захисту персональних даних у CRM-системі можна прийти до висновку, що базового захисту даних, які надають сучасні CRM-систем, більш ніж достатньо. Проте далеко не всі необхідні процедури захисту інформації можна реалізувати всередині CRM-системи.

Конкретний набір додаткових технічних засобів захисту необхідно визначати в кожному конкретному випадку, адже він буде залежати від загальної архітектури мережі, від архітектури конкретної CRM-системи та типів оброблюваної в ній інформації.

Висновки за розділом 2

В даному розділі було здійснено огляд найбільш використовуваних у системах управління відносинами з клієнтами архітектури: багаторівневої та мікросервісної архітектури.

Також було виконано аналіз методів захисту персональних даних у CRM-системі на прикладі системи Creatio. Методи захисту досліджувалися на таких рівнях функціонування системи:

- сервер додатків;
- сервер баз даних;
- сервер кешування Redis;
- сервер контролю версій (SVN);
- кінцеві станції користувачів.

Відповідно до здійсненого аналізу було визначено наступне:

а) базового захисту даних, які надають сучасні CRM-систем, більш ніж достатньо для підприємств малого та середнього масштабу;

б) для великих підприємств слід застосовувати додаткові технічні засоби захисту, перелік яких визначається в кожному конкретному випадку та залежить від загальної архітектури мережі, архітектури конкретної CRM-системи та типів оброблюваної в ній інформації;

в) виявлено недолік існуючого механізму журналювання змін даних в CRM-системі Creatio – система не журналює зміни, які були виконані на рівні СУБД (наприклад, при інтеграції на рівні СУБД).

РОЗДІЛ 3
РЕАЛІЗАЦІЯ НОВОГО МЕХАНІЗМУ ФІКСАЦІЇ ЗМІН ДАНИХ У СИСТЕМІ УПРАВЛІННЯ ВІДНОСИНАМИ З КЛІЄНТАМИ CREATIO

3.1 Політика здійснення правил розмежування доступу

Підприємства, які мають достатньо фінансових ресурсів, покладають процес впровадження CRM-системи у свою інфраструктуру на сторонні компанії, які на цьому спеціалізуються. Тож співробітники таких підприємств разом з безпосереднім впровадженням та налаштуванням системи надають її власникам та майбутнім користувачам рекомендації щодо здійснення правил розмежування доступу або налаштувань опцій системи, які будуть задовольняти конкретні вимоги з інформаційної безпеки.

До такого роду опцій відносяться, наприклад, налаштування кількості спроб вводу паролю, часу існування клієнтської сесії, перелік дозволених IP адрес тощо. Звісно, якщо це передбачено можливостями системи.

Зазвичай такими підприємствами є великі компанії з великим оборотом клієнтів, товарів та послуг, тому вони мають змогу крім придбання системи в базовій конфігурації наймати співробітників, які можуть вдосконалювати функції системи, в тому числі функції безпеки.

Організації, що відносяться до малого та середнього бізнесу частіше за все не мають таких можливостей, тому змушені задовольняти свої потреби безпеки лише тим набором налаштувань, які надаються в базовій конфігурації CRM-системи. Проте, відповідно до здійсненого в даній роботі аналізу на прикладі системи Creatio, можна прийти до висновку, що на сучасному ринку CRM-систем існують рішення, здатні забезпечити безпеку персональних даних на достатньому для малих підприємств рівні.

Будучи, можливо, недостатньо обізнаними у питаннях захисту інформації, власники таких систем, частіше за все ігнорують налаштування, що стосуються

безпеки, ставлячи для себе в пріоритеті залучення клієнтів та отримання від них прибутку, а не питання схоронності персональних даних цих клієнтів.

Як було зазначено у минулих розділах, розглядати в загальному вигляді технічні методи захисту всіх сучасних CRM-систем неможливо. Єдиним спільним компонентом системи усіх підприємств є співробітник, який працює з персональними даними клієнтів.

Практично будь-який проект впровадження CRM-систем здійснюється з початковим налаштуванням прав доступу для окремих користувачів чи групи користувачів всередині системи. Налаштування доступу можна здійснювати як для всієї таблиці, так і для окремих її записів або полів таблиці. Права роздаються на рівні бази даних, тому важливо забезпечувати захист серверів баз даних найбільш ефективно, оскільки отримання прямого доступу до бази даних надає користувачам доступ до всієї інформації в системі

Всі сучасні CRM-системи передбачають налаштування правил розмежування доступу, проте інтерфейси та певні налаштування у кожній окремій системі можуть відрізнятись.

Загальна інфраструктура середнього та великого бізнесу зазвичай складається к безлічі підсистем та додатків. Наприклад, в банківських структурах можливе наступне поєднання систем:

– CRM-система частіше за все виступає системою, з якою безпосередньо працюють співробітники відділень та офісів, яка компонує та систематизує дані, отримані з інших систем банку;

– автоматизовані банківські системи, які являються майстер-системами для зберігання даних договорів клієнтів та іншої банківської інформації;

– системи автоматизації функції банківського бек-офісу: управління платіжними картками, здійснення банківських транзакцій, обслуговування еквайрингових операцій тощо.

З точки зору кінцевих користувачів, кожен з співробітників працює лише в одній із систем та не має доступу до іншої. Так, наприклад, враховуючи типовий

алгоритм обслуговування клієнту у відділенні банку, процес заведення заявки та відкриття юридичною особою договору заробітного проекту має такі етапи:

а) менеджер відділення взаємодіє з CRM-системою, створює в ній заявку, та не супроводжує подальший процес її обробки;

б) співробітник головного офісу банку узгоджує параметри заявки в тій самій CRM-системі та формує договір заробітного проекту;

в) параметри заробітного проекту передаються в систему обліку роздрібних банківських операцій для випуску та обслуговування карток фізичних осіб.

Ще одним прикладом інфраструктури підприємства є уявна компанія «Клімат», яка здійснює продажі та обслуговування кліматичної техніки та використовує наступний алгоритм роботи:

– обробка замовлень, отриманих з 5 сайтів, на кожному з яких у день реєструється до 200 нових клієнтів та формується до 700 нових замовлень;

– відправлення в систему 1С сформованих в CRM-системі замовлень, для подальшого відвантаження;

– отримання з 1С статусів оплати і відвантаження замовлень;

– формування та відправка по e-mail «Рахунків на оплату» клієнтам;

– отримання актуальних даних по залишках товарів з 1С;

– прийом вхідних дзвінків, формування замовлень та звернень операторами контакт-центру;

– відображення в особистому кабінеті клієнта на сайтах історії та статусів звернень і замовлень;

– використання чат-ботів (наприклад, Viber та Telegram) для отримання статусів замовлень і звернень.

В цьому випадку загальна схема взаємодії підсистем підприємства, зображена на рис. 3.1, складається з певних компонентів та додатків, для обслуговування та адміністрування яких так само створюються різні робочі групи, кожна з яких має певний набір функціональних обов’язків, пов’язаних з конкретною системою.

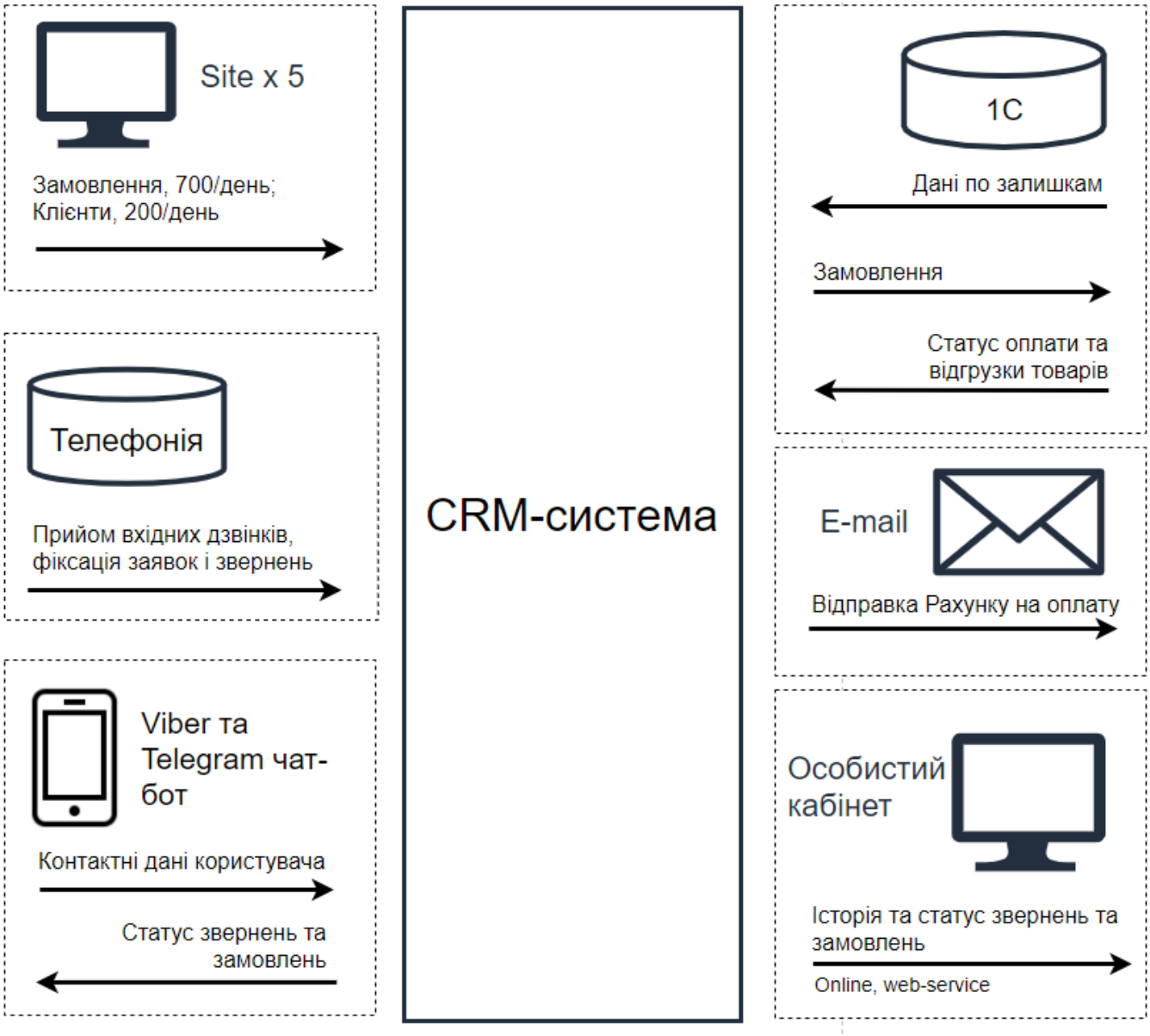

Рисунок 3.1 – Приклад схеми взаємодії підсистем підприємства

Такий підхід до організації розподілу обов'язків дозволяє зменшити ризик виходу систем з ладу, адже всі займаються тієї роботою, яку можуть робити найкраще.

Крім цього, обов'язково повинні існувати співробітники, які відповідають за всю інфраструктуру загалом. Це, в першу чергу, системні адміністратори, адміністратори та інженери інформаційної безпеки, адміністратори баз даних. Отже, варто зауважити, що для забезпечення належного рівня безпеки, здійснювати розподіл обов'язків та рівнів доступу співробітників слід таким чином, щоб їх функції не перетинались та були незалежними.

За такого підходу, у разі виникнення інциденту, пов’язаного зі зміною або видаленням даних у CRM-системі, першої лінією реагування на інцидент повинен бути співробітник, що являється адміністратором CRM-системи. Після чого він акумулює зібрану інформацію у певний звіт та передає ці дані адміністратору інформаційної безпеки для подальшого розслідування.

Як вже було зазначено у даній роботі, сучасні CRM-системи не функціонують окремо, а впроваджуються в існуючу інфраструктуру підприємства. Всередині цієї інфраструктури здійснюється передача даних від системи до системи, тому завжди існує ризик введення неправильних даних в одній системі, які згодом потраплять до системи CRM. Враховуючи, що система обслуговування клієнтів – це саме CRM-система, факт спотворення даних буде виявлений саме в ній. Тому дуже важливо відслідковувати ці зміни на рівні кожної окремої системи.

Співробітники CRM-системи, навіть адміністратори, не завжди мають доступ безпосередньо до бази даних, тому в даній роботі була поставлена задача реалізувати механізм фіксації та відображення змін даних безпосередньо у CRM-системі.

Приклад: менеджер відділення обслуговує клієнта та здійснює перевірку певних клієнтських даних. У разі, якщо клієнт виявляє розбіжності, немає необхідності одразу заводити інцидент інформаційної безпеки. Для з’ясування того, чи було це порушенням, якщо так, чи було воно здійснено в CRM, або певні клієнтські персональні дані були змінені в іншій системі та отримані вже такими, в першу чергу адміністратор самої CRM повинен здійснити аналіз логів та передати інцидент вже співробітнику інформаційної безпеки, якщо це необхідно.

Існуючий механізм журналювання змін CRM-системи Creatio, як було визначено вище, не дозволяє зафіксувати зміни, внесені в інших системах. Для цього необхідно виконувати журналювання на рівні бази даних. Враховуючи те, що співробітники CRM-системи безпосереднього доступу до БД не мають, було прийнято рішення реалізувати в CRM-системі Creatio механізм, який, по-перше, дозволяє фіксувати зміни в даних на рівні БД, та, по-друге, надати доступ до цієї інформації обмеженому колу співробітників CRM-системи для забезпечення

прозорості змін персональних даних та можливості розслідування інцидентів модифікації або видалення цих даних.

3.2 Ведення журналу змін даних в CRM-системі

Проект забезпечення безпеки веб-додатків OWASP являється стандартним документом про обізнаність розробників та безпеки веб-додатків. Він представляє собою широкий консенсус щодо найбільш критичних ризиків безпеки для веб-додатків [20].

Загалом, документом передбачено 10 найбільш критичних з точки зору інформаційної безпеки ризиків веб-додаткам:

– A1: ін’єкції. Види ін'єкцій, такі як SQL, NoSQL, OS та LDAP, виникають, у випадку, коли ненадійні дані надсилаються інтерпретатору як частина команди або запиту. Модифіковані дані зловмисника можуть змусити інтерпретатора виконувати некеровані команди або отримати доступ до даних без належного дозволу;

– A2: порушення автентифікації. Функції додатків, пов’язані з автентифікацією та управлінням сеансами, часто реалізуються неправильно, що дозволяє зловмисникам компрометувати паролі користувачів;

– A3: розголошення конфіденційних даних. Багато веб-додатків та API не захищають належним чином конфіденційну інформацію, таку як фінансові та ідентифікаційні дані. Тому зловмисники можуть викрасти їх або модифікувати для здійснення шахрайства з кредитними картками, викрадення особистих даних або інших злочинів. Крім цього, конфіденційні дані, для яких не використовуються криптографічні методи захисту, можуть бути так само скомпрометовані;

– A4: використання зовнішніх XML. Зовнішні сутності з використанням мови XML можна використовувати для розкриття внутрішніх файлів за допомогою обробника URI файлу, внутрішніх спільних файлів, внутрішнього сканування портів, віддаленого виконання коду та атак типу відмови в обслуговуванні;

– A5: порушення контролів доступу. Обмеження щодо того, що дозволено робити автентифікованим користувачам, часто здійснюється не належним чином.

Зловмисники можуть використовувати ці недоліки для доступу до конфіденційних даних, таких як доступ до облікових записів користувачів, перегляд конфіденційних файлів, зміна даних користувачів, зміна прав доступу тощо;

– A6: помилки в конфігурації безпеки. Зазвичай загрози такого типу є результатом небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та детальних повідомлень про помилки, що містять конфіденційну інформацію. Наприклад, у разі введення помилкового паролю користувачу може відобразитись такий текст помилки: «Для логіну A.Shved введено невірний пароль». Повідомлення такого роду неприпустимі, адже відображають логін користувача, до якого зловмисним може підібрати пароль;

– A7: міжсайтові сценарії XSS. Ризики використання XSS виникають у разі, коли система відображає дані користувачу на веб-сторінці без належної перевірки чи екранування. Ще одним способом прояву цієї загрози є оновлення веб-сторінки даними, наданими сторонніми системами за допомогою API браузера, який може створювати шкідливі HTML або JavaScript коди. Отже в загальному розумінні, міжсайтингові сценарії дозволяють зловмисникам виконувати шкідливі сценарії безпосередньо в браузері жертви. З точки зору захисту даних в CRM-системі цей ризик достатньо критичний, адже кінцеві користувачі працюють з системою безпосередньо зі своїх браузерів;

– A8: небезпечна десеріалізація. Така загроза частіше за все призводить до віддаленого виконання коду зловмисника на робочій станції жертви;

– A9: використання компонентів з відомими вразливостями. Вразливості, які є загальновідомими, можуть бути легко використані проти існуючих бібліотек, фреймворків та інших програмних модулів. Програми та API, які використовують компоненти з відомими вразливими місцями, можуть взагалі підірвати захист додатків та забезпечити різні атаки на всю систему;

– A10: недостатня реєстрація та моніторинг. Недостатня реєстрація та моніторинг у поєднанні з відсутністю реагування на інциденти інформаційної

безпеки дозволяє зловмисникам продовжувати атакувати систему, викрадати або знищувати дані.

Відповідно до пункту 10, недостатня реєстрація подій дозволяє зловмисникам продовжувати атакувати інформаційні системи. На прикладі CRM-системи, до такого роду ризику можна віднести ризик зміни конфіденційної інформації користувачів, здійснення модифікації даних, наприклад, кредитних карток. Не менш критичним ризиком є ризик втрати персональних даних клієнтів.

Також, оскільки в CRM-системах зберігаються персональні дані співробітників даних, важливо здійснювати моніторинг їх зміни задля зменшення ризиків, пов'язаних з викраденням паролів або фішингу. Без реалізації журналу змін даних відслідкувати, яка саме підсистема стала цьому причиною буде майже неможливо.

3.3 Практична реалізація механізму фіксації користувацьких дій

Існуючий мехінізм журналювання змін даних в CRM-системі Creatio має наступні можливості:

– налаштування правил журналювання для конкретного розділу (під розділом мається на увазі інтерфейсне зображення даних таблиці баз даних);

– можливість журанлювання додаткових полів, навіть тих, які не були змінені;

– налаштування підрахунку кількості змін в полях;

– підключення журналювання до будь-якого розділу системи і відображення різного набору полів для журналювання в залежності від сторінки редагування.

До недоліків існуючого механізму, виявлених в рамках даної роботи, відносяться:

– додаток не журналює зміни, які були виконані на рівні СУБД (наприклад, при інтеграції на рівні СУБД), що значно ускладнює процес відстеження змін персональних даних у разі виникнення інциденту – системний адміністратор CRM просто не зможе побачити зміни, а доступу до логів БД він не має.

Тож головним завданням було наступне: реалізувати механізм фіксації змін даних та відображення їх у CRM-системі для обмеженого колу осіб, який буде здійснювати фіксації змін даних, отриманих в тому числі шляхом імпорту даних зі сторонніх систем.

В рамках цієї роботи було розроблено алгоритм, за яким здійснюється фіксація змін даних у CRM-системі Creatio, а також реалізовано цей алгоритм у системі.

Отже, алгоритмом передбачено існування наступних організаційних та функціональних ролей у системі:

а) системний адміністратор CRM, який здійснює всі налаштування на має доступ до перегляду логів у системі CRM;

б) менеджер по роботі з клієнтами, який здійснює створення, модифікацію та видалення даних та не має доступу до перегляду логів у системі CRM.

Крок 1. Системний адміністратор створює налаштування журналювання (рис. 3.2), в якому вказує наступні параметри:

– назву об’єкту, зміни в якому необхідно фіксувати;

– код тригера, який буде згенеровано на обраному об’єкті;

– поля об’єкту, зміни в яких необхідно фіксувати (рис. 3.2), та додаткові поля;

– розділи системи, в яких будуть відображатись логи змін даних основного об’єкту, та перелік користувачів або ролей, яким ці записи будуть доступні (рис. 3.2).

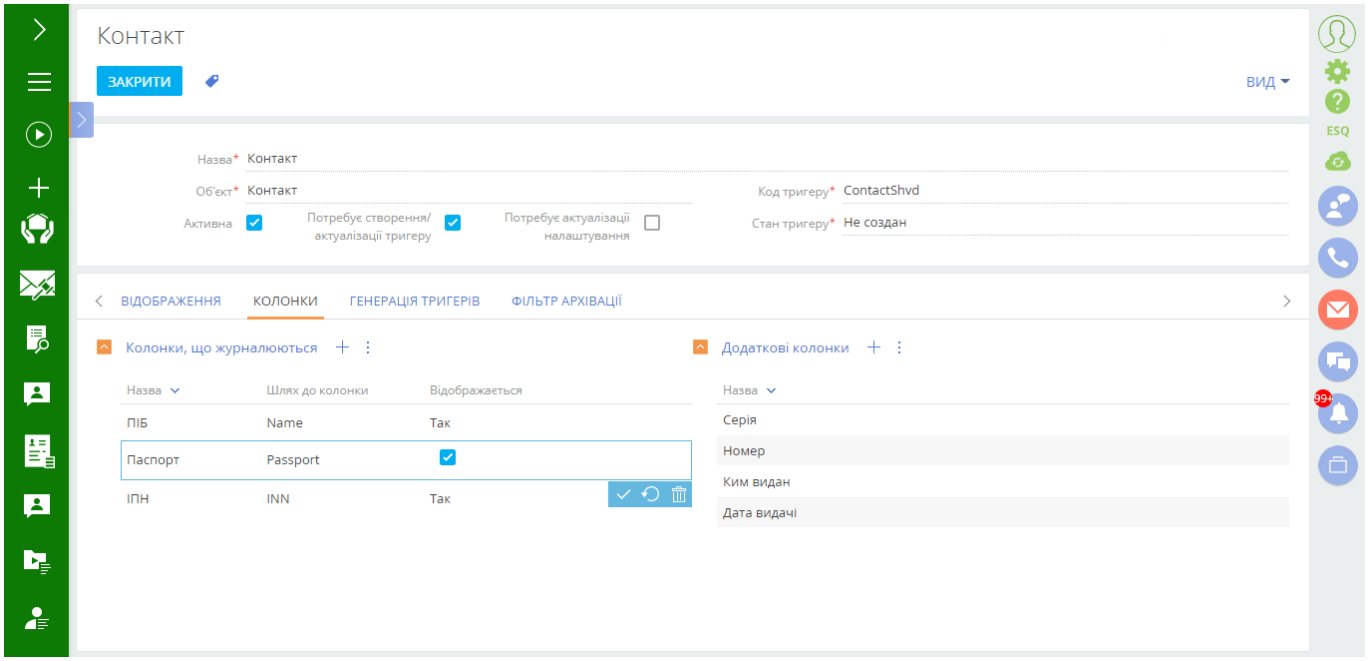

Рисунок 3.2 – Інтерфейс налаштування механізму журналювання у CRM-системі Creatio

Варто зазначити, що доступ до цих налаштувань також може бути обмежений організаційними та функціональними ролями.

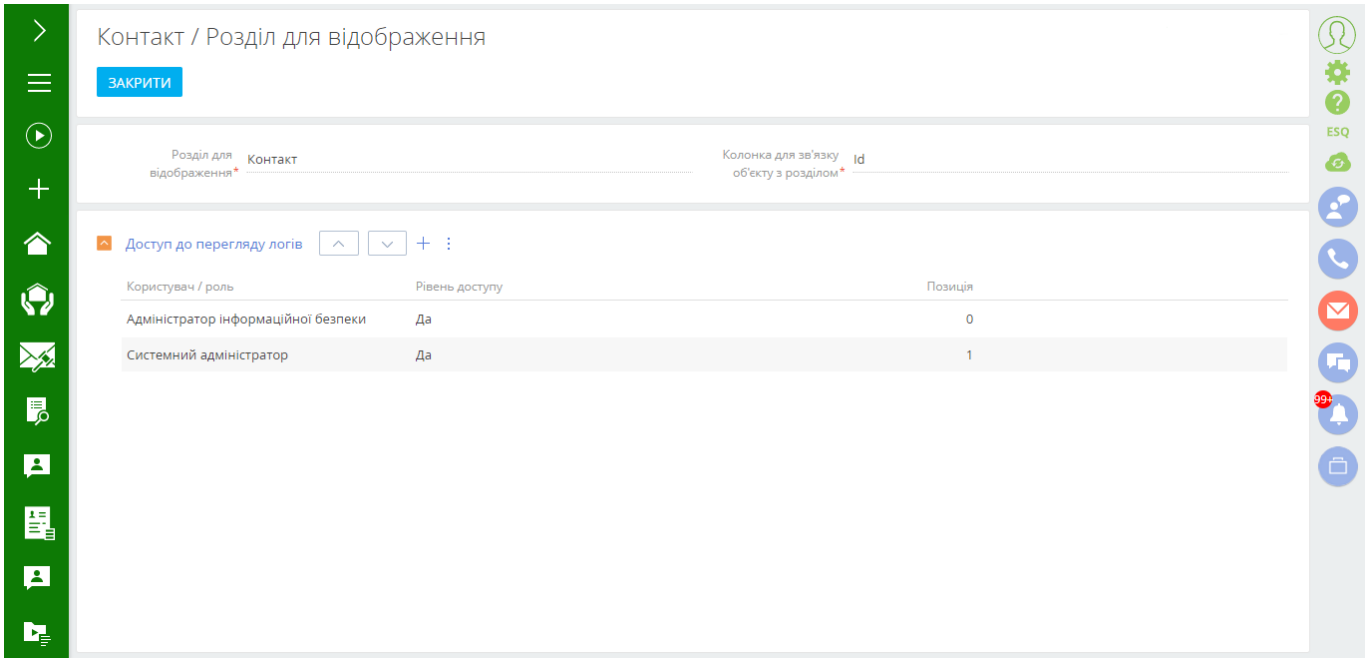

Рисунок 3.3 – Інтерфейс налаштування доступу до перегляду результатів журналювання у CRM-системі Creatio

Крок 2. Після збереження налаштування користувач має запустити процес створення тригеру на об’єкті в базі даних (рис. 3.4). Створений механізм передбачає, що користувач може забути активувати тригер, тому створене системне налаштування, яке запускає процес створення тригеру за розкладом.

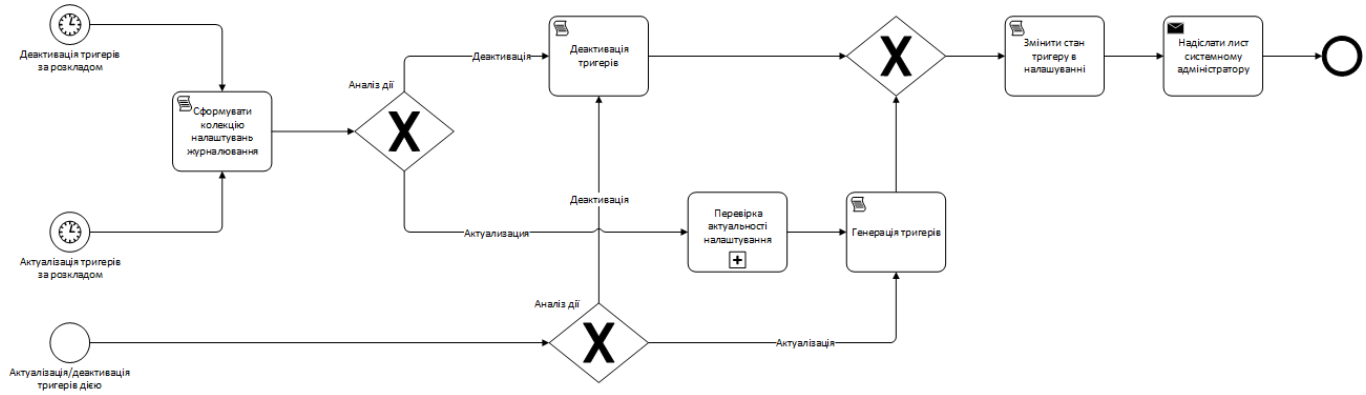

Рисунок 3.4 – Схема процесу актуалізації та деактивації тригерів

На рис. 3.4 схематично зображено процес актуалізації та деактивації тригерів. Відповідно до того, який показник стоїть в налаштуванні, відбувається або створення, або актуалізація, або деактивація тригеру.

В результаті на рівні бази даних буде створено три тригери на вказаний в налаштуванні об’єкт (рис. 3.5):

– INSERT – фіксує додавання даних;

– UPDATE – фіксує модифікацію даних;

– DELETE – фіксує видалення даних.

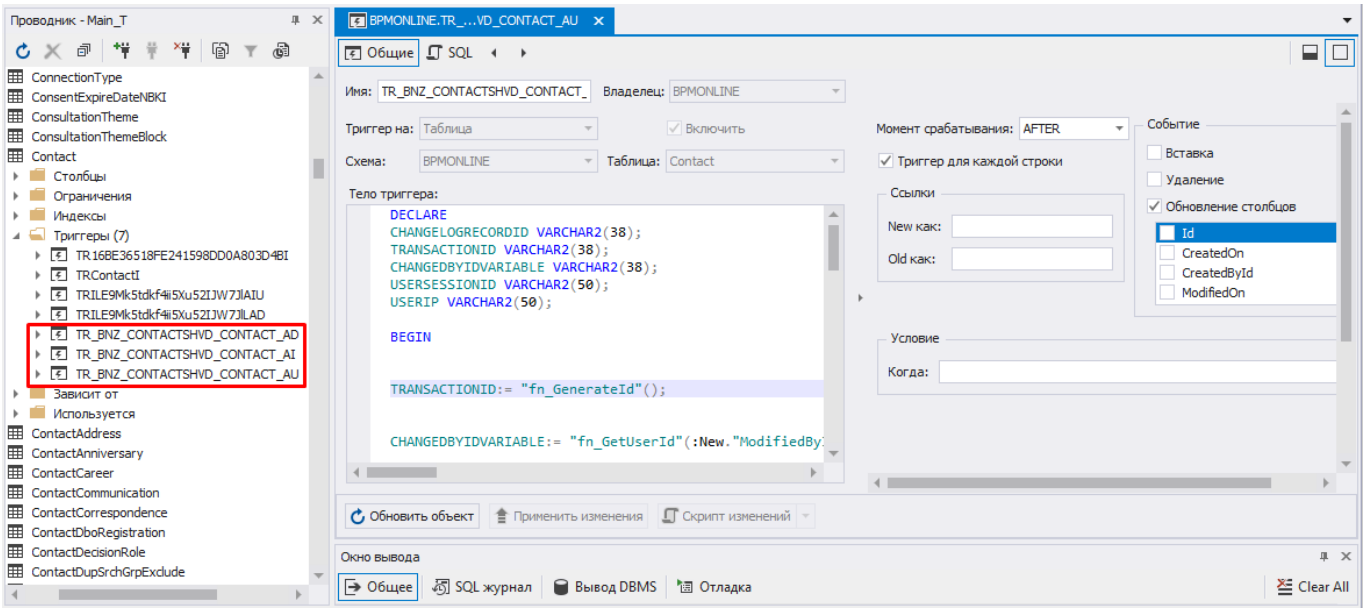

Рисунок 3.5 – Результат генерації тригерів фіксації змін даних у CRM-системі Creatio

Крок 3. Після додавання, зміни або видалення даних, системний адміністратор CRM або інший співробітник, який ще має на це доступ, може переглядати логи змін на сторінці (рис. 3.6) або в журналі змін (рис. 3.7).

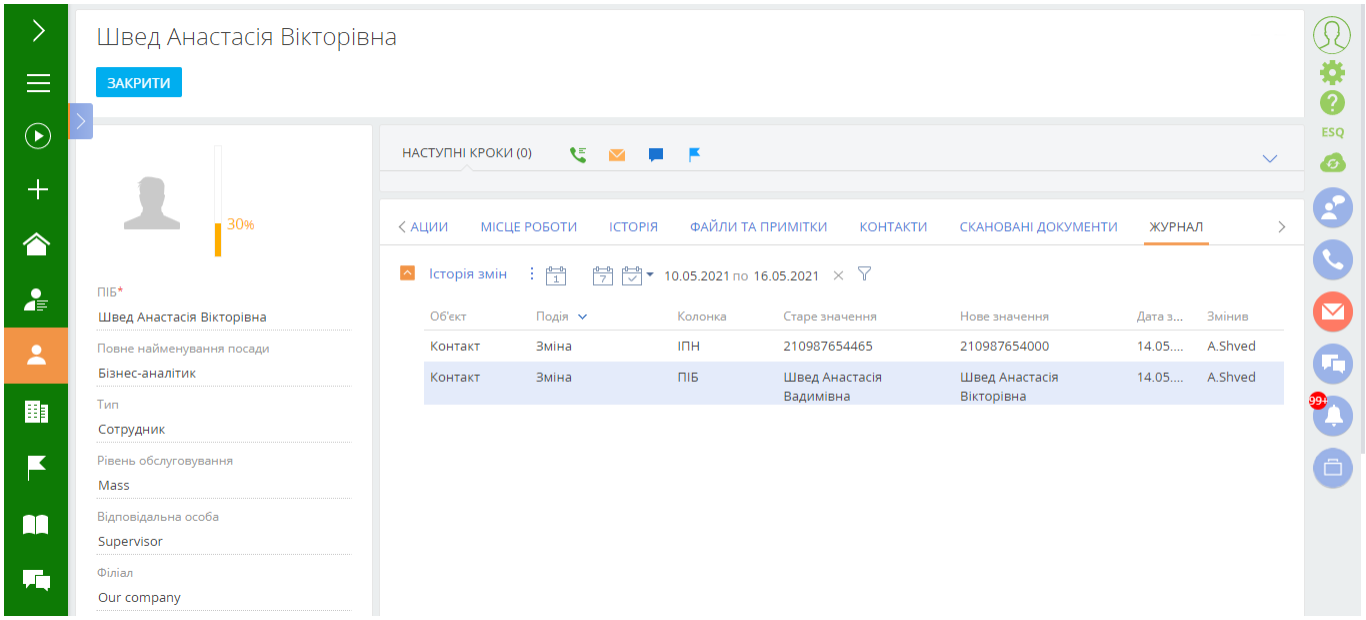

Рисунок 3.6 – Інтерфейс відображення логів зміни даних на сторінці CRM-системи Creatio

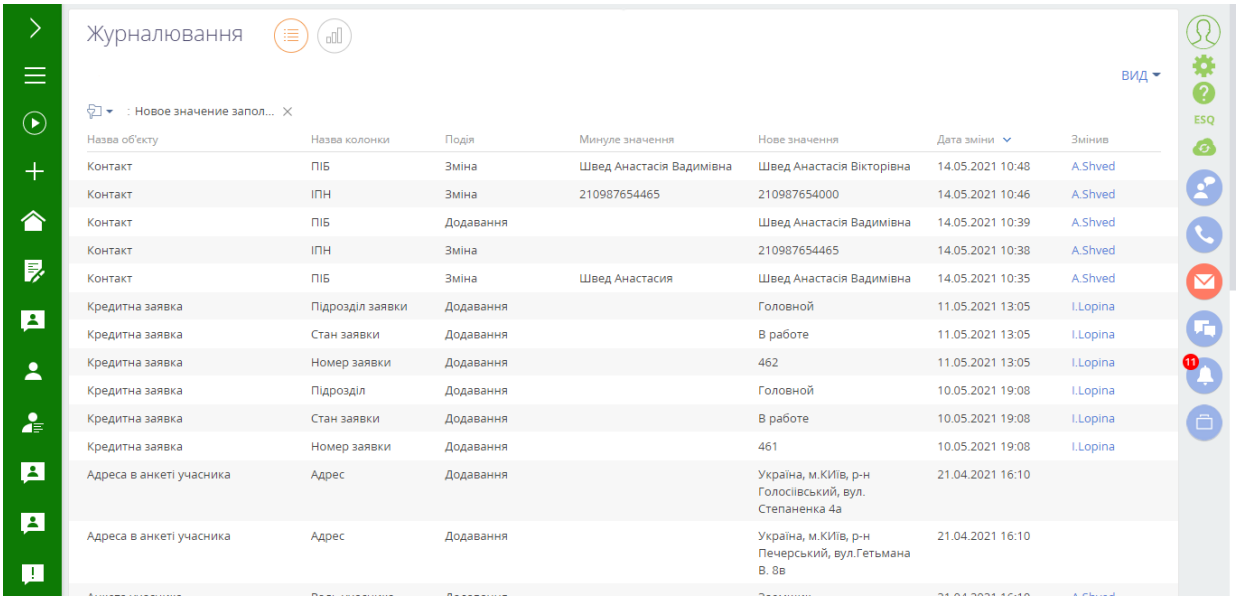

Рисунок 3.7 – Інтерфейс відображення логів зміни даних в журналі змін даних CRM-системи Creatio

Також передбачена архівація записів логу, адже велика кількість записів у таблиці, в яку пишуться факти журналювання змін впливає на продуктивність системи, що в свою чергу може негативно впливати на доступність даних у разі зависання системи. Механізмом передбачене задання налаштування фільтрації записів логу, які потрапляють в архів.

3.4 Переваги реалізованого механізму по відношенню до існуючого

Під час роботи та тестування розробленого механізму фіксації змін даних у CRM-системі Creatio було визначено, що новий механізм дозволяє здійснювати фіксацію змін, виконуваних безпосередньо в базі даних, на відміну від існуючого механізму.

Враховуючи те, що користувачі CRM-системи, в тому числі і її адміністратори, не мають безпосереднього доступу до таблиць бази даних, відстеження логів просто на рівні СУБД не покриває потреби безпеки персональних даних саме в CRM-системі, оскільки потребує залучення адміністратору баз даних до розслідування подій зміни або втрати даних.

Тож результатом роботи є вдосконалення такого методу захисту персональних даних в системі управління відносинами з клієнтами як моніторинг, ціллю якого є виявлення несанкціонованих дій, пов’язаних з обробкою інформації. Відповідно до міжнародного стандарту ISO/IEC 27001 даний механізм покриває критерій безпеки A.10.10 Моніторинг.

3.5 Рекомендації до застосування нового механізму CRM-системи Creatio та здійснення розподілу прав доступу

Оскільки даних механізм є елементом забезпечення безпеки персональних даних, в першу чергу необхідно обмежувати доступ до його налаштувань. Крім

цього, перегляд записів логів також повинен бути обмежений та недоступний звичайним користувачам системи.

З точки зору загальних правил до розподілу прав доступу у CRM-системі для забезпечення захисту персональних даних клієнтів, що зберігаються та обробляються у системі, власники CRM-систем повинні дотримуватись певних рекомендацій. Рекомендації надаються на прикладі CRM-системи Creatio.

Рекомендація №1: здійснювати розподіл організаційних та функціональних ролей.

Організаційна роль – це частина організаційної структури компанії, зазвичай певний підрозділ, наприклад, «Відділ продажів основного офісу» або «HR-відділ регіонального офісу».

Функціональна роль відображає посаду, яку співробітник займає в компанії, наприклад, роль «Менеджери з продажу».

Такий розподіл ролей дозволяє обмежувати права доступу для всього підрозділу або лише для деяких ролей в рамках цього підрозділу.

Рекомендація №2: використовувати різні типи доступу.

У системі Creatio бізнес-дані зберігаються у вигляді записів в різних об’єктах. Тобто кожному розділу системи (рис. 3.8), деталі (рис. 3.9), довіднику (3.10) та іншому бізнес-об'єкту системи відповідає певний об'єкт в базі даних. Об'єкти, в свою чергу, відповідають таблицями в базі даних.

Управління доступом до даних має на увазі управління правами доступу до цих об'єктів. Права доступу на об'єкти можна обмежити на трьох рівнях:

- за операціями, а саме:
    1) читання;
    2) зміна;
    3) видалення;
- за записами;
- по колонках.

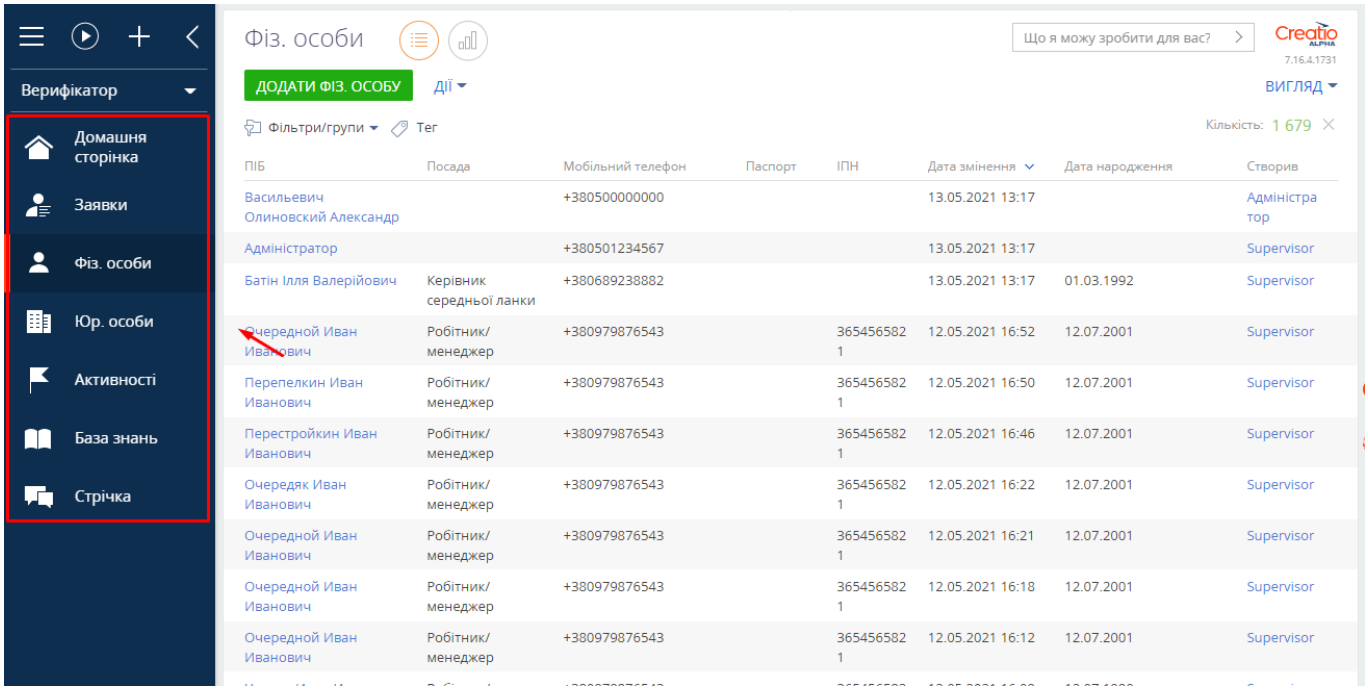

Рисунок 3.8 – Інтерфейс CRM-системи Creatio. Роділи

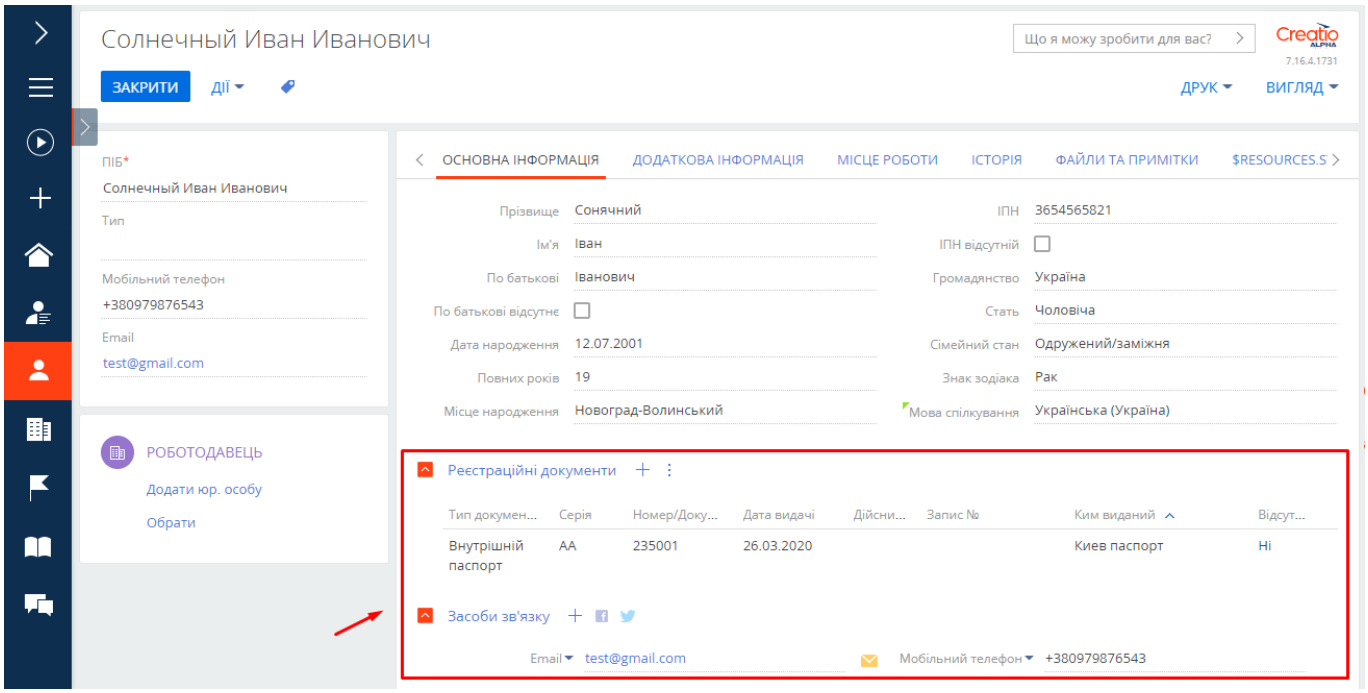

Рисунок 3.9 – Інтерфейс CRM-системи Creatio. Деталь

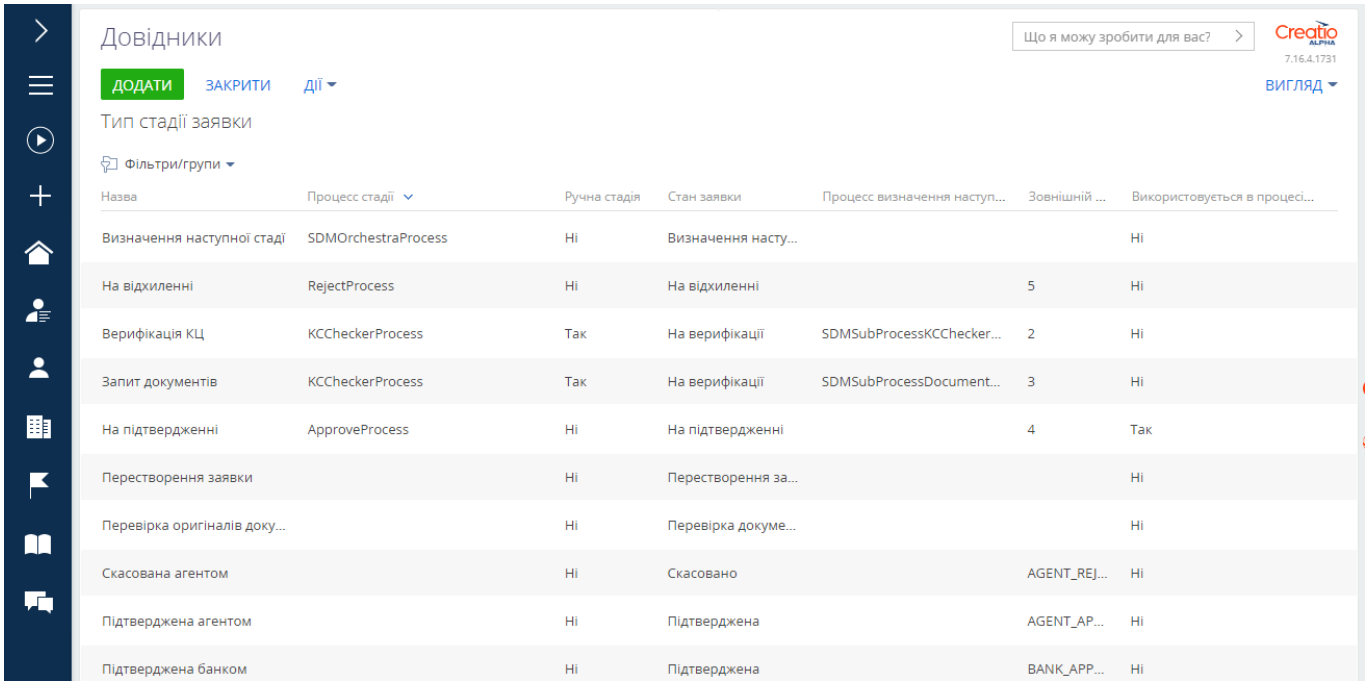

Рисунок 3.10 – Інтерфейс CRM-системи Creatio. Довідник

Рекомендація №2.1: здійснення розмежування прав доступу на об’єкти (по операціям).

Цей варіант адміністрування доступу дозволяє надати або обмежити права на читання, створення, редагування і видалення даних об'єкта (CRUD-операції) для окремих користувачів або ролей.

В системі Creatio існує ознака «Доступ за операціями обмежений» на кожному з об’єктів. Якщо вона не встановлена, то всі користувачі мають можливість переглядати, створювати, редагувати і видаляти всі записи в об'єкті.

Не рекомендується надавати доступ всім користувачам до всієї інформації системи.

Встановлення ознаки «Доступ за операціями обмежений» означає, що можливість виконання CRUD-операцій в об'єкті буде тільки у тих користувачів і ролей, яким таке право було спеціально надано. Решта користувачів і ролі (за винятком системних адміністраторів) не матимуть доступ до об'єкта. Наприклад, тільки окремі користувачі можуть додавати нові записи. Користувачі і ролі, для яких не налаштований доступ за операціями до такого об'єкта, не зможуть бачити, додавати, змінювати або видаляти його дані.

Рекомендація №2.2: здійснення розмежування прав доступу на записи.

Цей варіант адміністрування доступу дозволяє управляти правами на читання, редагування і видалення окремих записів обраного об'єкта, а також на делегування цих прав. За замовчуванням доступ до нового запису є тільки у її автора. Автор запису може самостійно налаштовувати права доступу до неї для інших користувачів.

Рекомендується такі налаштування надавати лише системному адміністратору на здійснювати наступним чином:

– записи, створені користувачами одного підрозділу, повинні бути доступні для читання в рамках цього самого підрозділу, якщо інше не передбачене встановленими на підприємстві процесами;

– видалення записів, створених користувачем, повинні бути доступні лише цьому користувачеві, його керівнику та системному адміністратору.

Системою Creatio також передбачено здійснення розмежування прав доступу на колонки. Цей варіант адміністрування доступу дозволяє управляти правами на окремі поля об’єкту. Проте на практиці не рекомендується встановлювати ці налаштування, адже це значно впливає на продуктивність системи на рівні баз даних.

Рекомендація №3: розмежування прав на здійснення операцій, які не відносяться до конкретного об’єкту.

Наприклад, в CRM-системі Creatio для цього передбачено так зване налаштування прав доступу на системні операції, в якому системний адміністратор може так само зазначати перелік ролей або користувачів, які мають права на виконання тих чи інших дій.

Гарним прикладом операції, на яку обов’язково треба налаштовувати права, є операція імпорту даних, задля мінімізації ризику витоку конфіденційної інформації. Також системними операціями зазвичай регулюєтеся доступ до конфігураційних налаштувань системи.

Рекомендація №4: налаштування окремих системних робочих місць.

Як вже було зазначено вище, у CRM-системах, в тому числі і Creatio, існують так звані розділи, які по суті являються інтерфейсним відображенням даних таблиць БД.Такий розподіл впливає лише на відображення того чи іншого розділу тому чи іншому користувачу.

За умови здійснення правильного налаштування на рівні об’єктів, користувач, що не має права, наприклад, на видалення або модифікацію даних не зможе завдати ніякої шкоди у разі отримання доступу до перегляду цього об’єкту. Проте факт порушення конфіденційності даних завжди може мати місце.

Отже, підходити до питання здійснення розмежування прав доступу на об’єкти системи, в яких зберігаються персональні дані користувачів, слід дуже ретельно. Що важливо, робити це необхідно на етапі проектування системи. Лише такий підхід та використання наданих рекомендацій дозволить мінімізувати ризики персональним даним в системах управління відносинами з клієнтами, які можуть бути спричинені умисними або не умисними діями користувачів системи.

Висновки за розділом 3

В даному розділі було удосконалено та реалізовано механізм фіксації змін даних у системі управління відносинами з клієнтами Creatio. У порівнянні з існуючою у системі логікою журналювання змін, новий механізм дозволяє:

- налаштовувати перелік об’єктів, зміни даних в яких необхідно фіксувати;
- відображати логи змін безпосередньо в інтерфейсі системи;
- регулювати права доступу на перегляд створених логів;
- здійснювати фіксацію змін, виконуваних безпосередньо в базі даних, на відміну від існуючого механізму.

Також в розділі 3 було надано практичні рекомендації щодо впровадження створеного механізму та рекомендації щодо здійснення прав розмежування доступу у системі управління відносинами з клієнтами на прикладі системи Creatio.

ВИСНОВКИ

Метою роботи було удосконалення існуючих методів захисту персональних даних у системах управління відносинами з клієнтами.

Для досягнення поставленої цілі було здійснено визначення рівня критичності такого активу підприємств як клієнтська база. Доведено, що персональні дані клієнтів
є одним з важливих інформаційних активів підприємства, який потребує великих капіталовкладень та дозволяє компанії отримувати прибуток зі своєї операційної діяльності.

В роботі було визначено ключові загрози порушення основних властивостей інформації, що складає собою персональні дані клієнтів. Відповідно до здійсненого аналізу інцидентів інформаційної безпеки та за результатами процедури ризик-менеджменту було визначено, що в силу наявності у співробітників компанії безпосереднього доступу до системи, більшість з описаних порушень є наслідками людських дії та помилок, які достатньо складно передбачити при розробці системи.

На прикладі системи Creatio, розробленої компанією Terrasoft, було здійснено аналіз методів захисту даних, які надають сучасні системи управління відносинами з клієнтами.

Відповідно до цього огляду було отримано висновок, що для більшості підприємства базового захисту даних, які надають сучасні CRM-систем, більш ніж достатньо. Для великих підприємств рекомендується також застосовувати додаткові технічні засоби захисту, перелік яких визначається в кожному конкретному випадку та залежить від загальної архітектури мережі, архітектури конкретної системи управління відносинами з клієнтами та типів оброблюваної в ній інформації

Було виявлено, що існуючий у CRM-системі Creatio механізм журналювання змін даних не покриває потреби у фіксації змін даних шляхом здійснення інтеграцій на рівні баз даних. Це є ключовим моментом у питанні реєстрації змін даних у підприємствах, системах управління відносинами з клієнтами яких є лише одним із

компонентів загальної інфраструктури, в якій передбачається передача даних від однієї системи до іншої.

Реалізований новий механізм журналювання змін даних в системі управління відносинами з клієнтами Creatio успішно виконує поставлені задачі та являється більш досконалим за існуючий механізм системи.

В кінці роботи було надано загальні рекомендації щодо розмежування прав доступу на прикладі системи управління відносинами з клієнтами Creatio.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Customer Acquisition Cost: How to Calculate, Reduce & Improve It. URL: https://neilpatel.com/blog/customer-acquisition-cost

2. Как растет и развивается monobank. URL: https://ain.ua/2020/10/07/kak-razvivayetsya-monobank-forbes

3. Monobank запустил крупнейшую рекламную кампанию в истории бренда. URL: https://ain.ua/2020/07/03/reklamnaja-kampanija-monobank

4. Управління відносинами з клієнтами. URL: https://uk.wikipedia.org/wiki/Управління_відносинами_з_клієнтами

5. Rodionov Serhii O. A study on theoretical aspects of developing systems for customer relationship management as an alternative direction of development of the marketing activity for machine-building enterprises. *БИ*. 2015. № 10

6. Про захист персональних даних: Закон України від 23.02.2012 р. №4452-VI. Дата оновлення: 30.01.2021. URL: https://zakon.rada.gov.ua/laws/show/2297-17

7. General Data Protection Regulation, GDPR. URL: https://gdpr-info.eu

8. Lainhart IV J. W. COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems*. 2000. Т. 14. № 1. С. 21–25.

9. Кулик Ю. М. Сучасне трактування та функції ризик-менеджменту підприємства. *Економічний форум*. 2016. №. 4. С. 158–163.

10. BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz.

11. Дмитрієв А.А.: Ризик-менеджмент за вимогами міжнародного стандарту ISO/IEC 27001. Один із способів побачити майбутнє без машини часу. *Das Менеджмент*. 2010. № 4. С. 79–83.

12. NIST 800-30. Risk management guide for information technology systems.

13. Verizon Data Breach Investigations Report 2020. URL: https://www.verizon.com/business/resources/reports/dbir/

14. Verizon Data Breach Investigations Report 2017. URL: https://www.verizon.com/business/resources/reports/dbir

15. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

16. HAProxy. URL: http://www.haproxy.org

17. CRM-система Creatio. URL: https://www.terrasoft.ua/page/crm-products

18. IIS. URL: https://www.iis.net

19. Нечипоренко, О. В., Міценко С. А. Механізми забезпечення захисту баз даних в сучасних СУБД. *Вісник Черкаського державного технологічного університету. Технічні науки*. 2014. №3. С. 80–86.

20. OWASP Top Ten. URL: https://owasp.org/www-project-top-ten.

ДОДАТОК А

АРХІТЕКТУРА СИСТЕМИ УПРАВЛІННЯ ВІДНОСИНАМИ З КЛІЄНТАМИ НА ПРИКЛАДІ CRM-СИСТЕМИ CREATIO

The abstracts of the report describe the main functions of modern CRM-systems (Customer Relationship Management). On the example of the Creatio system the typical scheme of the CRM-system architecture is considered and the analysis of its key components is carried out

Key words: *Customer Relationship Management system Creatio; architecture of CRM-system Creatio; horizontal scaling.*

Сьогоденне збільшення кількості товарів та послуг призводить до зростання конкуренції серед підприємств та виникнення нових способів утримання конкурентної переваги і збільшення прибутку. Саме тому організації намагаються залучати нових клієнтів та утримувати вже існуючих. Звичайно, зі збільшенням кількості споживачів повинна зростати і кількість менеджерів по роботі з клієнтами, але не всі компанії можуть собі дозволити збільшувати штат відповідно до зростання кількості клієнтів. Це призводить або до зменшення швидкості обслуговування клієнтів, або до зниження якості роботи менеджерів. Обидва варіанти дуже негативно впливають на репутацію підприємства, що зрештою призводить до ще більшого зменшення кількості споживачів товару або послуг та зниження прибутків організації.

Системи управління відносинами з клієнтами призначені для збору, зберігання й аналізу інформації про споживачів, а також для автоматизації споживчих бізнес-процесів, що допомагає персоналу з роботи з клієнтами виконувати свої функції швидше та ефективніше [1].

Базові можливості CRM-системи Creatio дозволяють збирати всю інформацію про клієнтів та контрагентів в єдиній системі, актуалізувати її з відкритих джерел, за допомогою інтеграцій зі сторонніми системами; гнучко налаштовувати весь цикл

продажів та створювати каталог всіх продуктів чи сервісів з повним набором їх характеристик та особливостей; використовувати єдине вікно операторів контакт-центру, яке дозволяє користувачам виконувати всі свої робочі функції, не переключаючись між розділами системи [2].

Незважаючи на великий список можливостей CRM-системи (як Creatio, так і будь-якої іншої представленої на ринку), підприємства частіше за все вдаються до розширення існуючих функцій системи та підлаштовують її до власних потреб. CRM-система Creatio дозволяє користувачам на своїй платформі здійснювати користувацьку розробку, що зобов'язує її власників розуміти не лише інтерфейсну частину додатку, а й всю її архітектуру для того, щоб не призвести своїми діями до відмови в роботі системи.

На прикладі CRM-системи Creatio розглянемо два можливі способи побудови такої системи – схему архітектури для задоволення потреб малого бізнесу та схему архітектури з використанням горизонтального масштабування для великих організацій з великою кількістю користувачів.

Розглянемо типову схему архітектури CRM-системи Creatio, що представлена на рис.1.

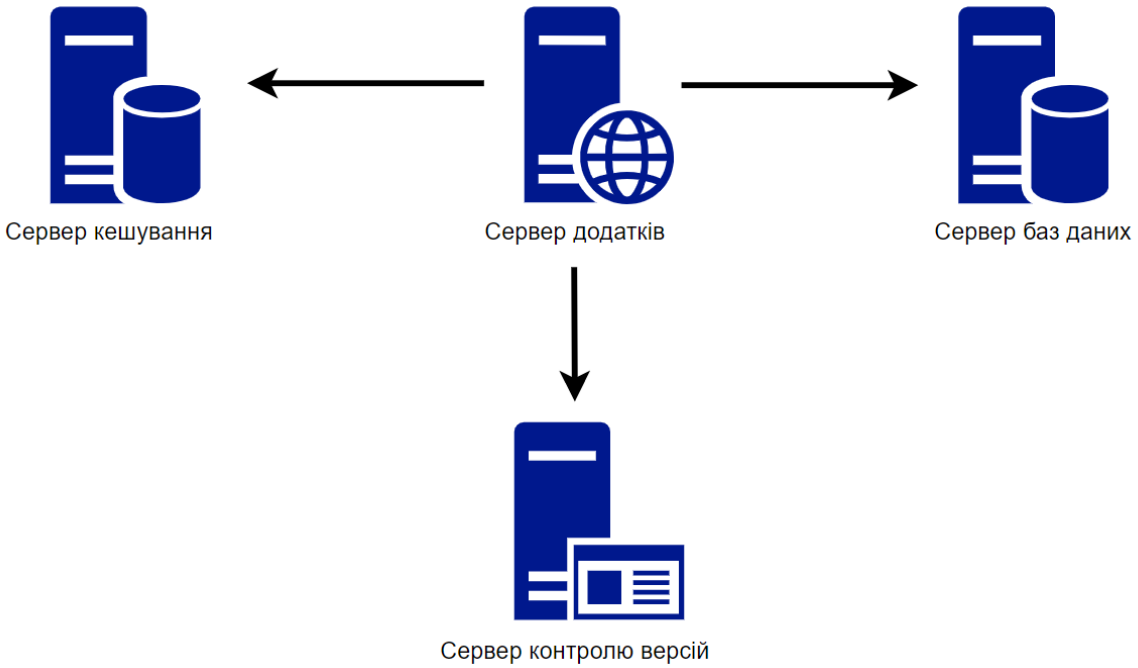

Рис. 1. Схема архітектури основного додатку Creatio

Така типова схема може бути використана на підприємствах з невеликою кількістю користувачів (близько 20 – 100) та не потребує значних витрат на потужні сервери – достатньо використання лише трьох обов'язкових виділених серверів: серверу додатків, серверу баз даних та серверу кешування. Сервер контролю версій в даному випадку є опціональним компонентом схеми та використовується лише у випадку, коли існує багатокористувацька розробка додаткового функціоналу системи.

Сервер додатків виконує основну обчислювальну роботу системи. Додаток на платформі .NET Framework працює під управлінням Internet Information Services (IIS) та складається з завантажувача (WebAppLoader) і конфігураційної частини (WebApp).

Основне призначення завантажувача – виконання службових функцій системи, і подальше перенаправлення користувачів в основну програму Creatio. Після обробки в завантажувачі запиту на авторизацію, користувачі можуть працювати в конфігураційній частині – програмі, яка відповідає за роботу бізнес-логіки системи.

Сервер баз даних. В базі даних додатку зберігаються користувацькі дані, дані, необхідні для роботи системи та конфігураційні налаштування. Найбільш використовуваними системами управління баз даних Creatio є MS SQL Server або Oracle. Також система підтримує PostgreSQL [3].

Сервер кешування Redis відповідає за зберігання даних користувача і додатку (профіль користувача, сесійні дані тощо), зберігання кешованих даних, обмін даними між вузлами веб-ферми.

Redis підтримує такі стратегії зберігання даних [4]:

- зберігання даних лише в пам'яті;
- періодичне збереження даних на диск (за замовчуванням);
- лог транзакцій;
- реплікація.

В Creatio зберігання даних здійснюється в пам'яті з періодичним збереженням дампу на диск [3].

Як вже було зазначено раніше, великим підприємствам недостатньо базової функціональності системи Creatio, тому компанії намагаються власними силами або через посередників розширювати функціонал системи. **Сервер системи контролю версій** є опціональним компонентом додатку та використовується саме у тому випадку, коли паралельно з експлуатацією системи необхідно на платформі організувати розробку користувальницької конфігурації.

Відповідно до того, які завдання ставить підприємство перед CRM-системою, зростають і її масштаби; відповідно до величини підприємства визначається й кількість співробітників, які будуть використовувати систему.

Для CRM-системи організації, що складається з великих бізнес-процесів, які виконують складні, ресурсномісткі функції, та кількість користувачів якої сягає понад 100, 200 або навіть 1000 користувачів, використання одного серверу додатків, одного серверу баз даних та серверу кешування вже не буде достатнім для забезпечення безперервної та стабільної роботи системи.

В такому випадку, підвищити продуктивність великих проектів дозволяє горизонтальне масштабування системи. При цьому схема архітектури системи Creatio (рис. 2) приймає наступний вигляд:

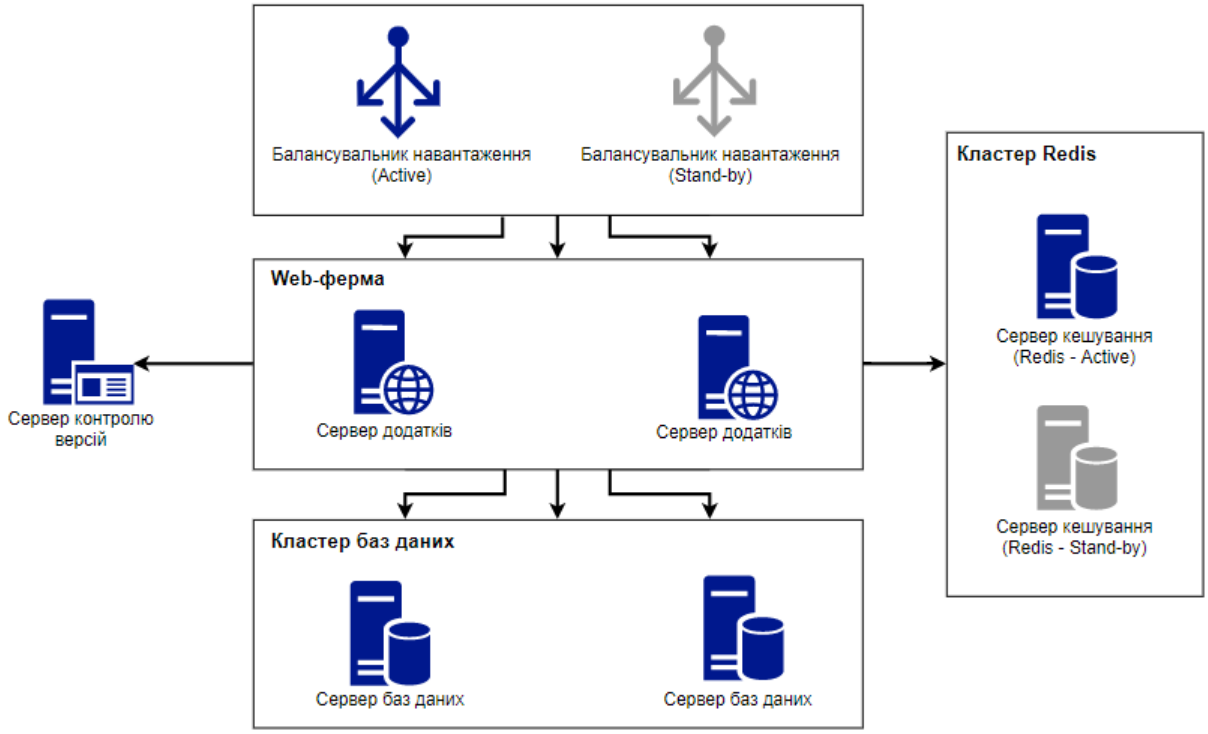

Рис. 2. Схема архітектури основного додатку Creatio при використанні горизонтального масштабування

При використанні горизонтального масштабування обов'язковим компонентом системи є балансувальник навантаження, який може бути як програмним, так і апаратним. У системі Creatio для роботи у відмовостійкому режимі використовується балансувальник HTTP / HTTPS-трафіку з підтримкою протоколу WebSocket – HAProxy. Балансувальник HAProxy підримує такі операційні системи як Linux, FreeBSD, OpenBSD, Solaris, AIX та являється програмою з відкритим кодом, що дозволяє переконатися у відсутності вразливостей додатку [3].

Для більшої надійності системи балансувальник навантаження працює в режимі Active / Stand-by, тобто один з балансувальників знаходиться в активному режимі, інший – в режимі очікування; у разі виникнення проблем в активній системі, її роботу заміняє резервна система, поки проблема не буде вирішена.

Крім цього, якщо кількість користувачів системи налічує декілька тисяч, звичайні сервери додатків, сервер баз даних та сервер кешування Redis замінюються серверною Web-фермою, кластером баз даних та кластером Redis, відповідно. Такий підхід до реалізації дозволяє мінімізувати відмови в роботи системи.

Розглянувши схему архітектури CRM-системи на прикладі Creatio можна прийти до висновку, що сучасні системи управління відносинами з клієнтами забезпечують гнучкий підхід до вирішення і автоматизації завдань конкретної організації. А використання горизонтального масштабування дозволяє великим підприємствам налагоджувати свої бізнес-процеси без страху втратити при цьому продуктивність системи.

ЛІТЕРАТУРА

1. Шовкопляс С. Как повысить конкурентоспособность при помощи CRM // Office. − 2005. − № 3-4. − с. 12-18

2. Опис CRM-системи Creatio [Електронний ресурс] – Режим доступу: https://www.terrasoft.ru/page/crm-products.

3. Документація Creatio Terrasoft [Електронний ресурс] – Режим доступу: https://academy.terrasoft.ru/documentation.

4. Документація Redis [Електронний ресурс] – Режим доступу: https://redis.io/documentation.