Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Організація захисту персональних даних в підприємстві ТОВ <ЕСКО ><ЕКО-ІДЕЯ>
Назва теми

КвРКБ.170147.17.01.09 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Назва

Виконав: студент IV курсу, група КБ–17–1 Н.О. Мироненко
Підпис Ініціали, прізвище

Керівник _____ І.В. Муляр
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.В. Муляр
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки та
комп'ютерних систем і мереж _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

«23» червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Завідувач кафедри _____

_____

5.02 •2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мироненку Назару Олександровичу

Прізвище, ім'я, по батькові студента

1 Тема роботи Організаціязахиступерсональнихданих в підприємстві ТОВ <ЕСКО ><ЕКО-ІДЕЯ>

Керівник роботи _____

_____

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від05022021р. №11 додаток 9

2 Строк подання студентом роботи на кафедру:_____

3 Вихідні дані до роботисистеми запобігання та виявлення витоків даних, , методи аналізу та захисту персональних даних, криптографічні засоби захисту інформації_____

4Зміст пояснювальної записки (перелік питань, які потрібно розробити) Аналіз об'єкта захисту, обгрунтування вибору засобів для побудови системи безпеки, проектування системи безпеки, реалізація роботи_____

_____

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «Алгоритм роботи модуля мережевої активності», «Алгоритм роботи модуля виявлення атак», «Алгоритм роботи модуля обробки даних», «Архітектура системи захисту персональних даних», «Архітектура системи захисту персональних даних модифікована.

6 Консультанти розділів курсового проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Муляр І.В., доцент кафедри КбКСМ		
Антиплагіат	Муляр І.В., доцент кафедри КбКСМ		

7 Дата видачі завдання _____ _____ 20___р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір та затвердження теми кваліфікаційної роботи.	Січень	–
2	Аналіз об'єкта захисту.	Січень–лютий	–
3	Проектування та розробка загальної архітектури і структури системи захисту.	Лютий–березень	–
4	Програмна реалізація запропонованого рішення та тестування системи; аналіз результатів і оцінювання прийнятих рішень.	Квітень	–
5	Написання тексту пояснювальної записки та розробка графічних матеріалів.	Травень	–
6	Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника.		–
7	Оформлення кваліфікаційної роботи як документа відповідно до вимог.		–
8	Отримання супровідних документів. Нормоконтроль.	Червень	–
9	Підготовка до захисту та захист кваліфікаційної роботи.		–

Студент _____ Н.О.Мироненко
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ І.В. Муляр
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Організація захисту персональних даних в підприємстві ТОВ <ЕСКО ><ЕКО-ІДЕЯ>».

Автор роботи: Мироненко Назар Олександрович.

Керівник роботи: Муляр Ігор Володимирович.

Обсяг – 49 с., 11 рис., 2 додатка, 18 джерел.

Графічна частина: 9 презентаційних слайдів, 5 плакати.

Організація захисту персональних даних в підприємстві ТОВ <ЕСКО><ЕКО-ІДЕЯ>.

Метою роботи є вивчення та аналіз типових проблем інформаційної безпеки пов'язаних із витоком даних, побудова системи захисту персональних даних, що може здійснювати відслідковування даних в середині інформаційного простору компаній і виявляти неправомірні дії користувачів системи над нею.

У роботі було проаналізовано та досліджено типові проблеми інформаційної безпеки в кібернетичному просторі, особливу увагу було зосереджено на проблемі витоків даних із конфіденційною інформацією причиною якого є внутрішній порушник інформаційної безпеки.

В рамках кваліфікаційної роботи була розроблена система захисту персональних даних, спроектована із врахуванням побажань співробітників ТОВ <ЕСКО ><ЕКО-ІДЕЯ>.

Підпис студента

07.06.2021
Дата

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1		Завдання на дипломний	1	
				проект		
А4		2		Анотація	1	
А4		3	КвРКБ.170147.17.01.09 ПЗ	Організація захисту	1	
				персональних даних		
				в підприємстві		
				ТОВ <ЕСКО ><ЕКО-ІДЕЯ>		
				Пояснювальна записка		
А3		4	КвРКБ.170147.17.01.09 Е8	Архітектура системи	1	
				захисту персональних даних		
				витоків даних		
				Схема структурна		
А3		5	КвРКБ.170147.17.01.09 Е8	Архітектура системи	1	
				захисту персональних даних		
				модифікована		
				Схема структурна		
А3		6	КвРКБ.170147.17.01.09 Е8	Робота модуля	1	
				мережевої активності		
				Алгоритм роботи		

Зм.	Арк.	№ Докум.	Підп.	Дата	КвРКБ.170147.17.01.09 ВП		
Розробив		Мироненко Н.О.			Організація захисту персональних даних в підприємстві ТОВ <ЕСКО><ЕКО-ІДЕЯ> Відомість проекту	Літера	Аркуш	Аркушів
Перев.		Муляр І.В.				н	1	2
Н. контр.		Муляр І.В.				ХНУ, КБ-17-1		
Затв.		Кльоц Ю.П.						

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
A2		7	КвРКБ.170147.17.01.09 Е8	Робота модуля	1	
				виявлення атак		
				Алгоритм роботи		
A2		8	КвРКБ.170147.17.01.09 Е8	Робота модуля	1	
				обробки даних		
				Алгоритм роботи		

Зм.	Арк.	№ Докум.	Підп.	Дата	КвРКБ.170147.17.01.09 ВП	Арк. 2

ЗМІСТ

ВСТУП

Повсюдна комп'ютеризація, що почалася в кінці XX століття триває і в наші дні. Автоматизація процесів в організації підвищує продуктивність праці співробітників організації. Користувачі інформаційних систем можуть швидко отримувати дані необхідні для виконання їх посадових обов'язків. Однак разом з полегшенням доступу до даних існує проблеми збереження цих даних. Володіючи доступом до різних інформаційних систем, зловмисники можуть використовувати їх в корисливих цілях: збір даних для продажу їх на чорному ринку, крадіжка грошових коштів у клієнтів організації, крадіжка комерційної таємниці організації.

Тому проблема захисту критично важливої інформації для організацій стоїть дуже гостро. Все частіше стає відомо зі ЗМІ про різну техніку або методиках крадіжки грошових коштів шляхом злому інформаційних систем фінансових організацій. Отримавши доступ до інформаційних систем персональних даних, зловмисник може поцупити дані клієнтів фінансових організацій, інформацію про їх фінансові операції поширити їх, завдавши клієнту як фінансовий, так і репутаційну шкоду. Крім того, дізнавшись дані про клієнта, шахраї можуть напряму подзвонити клієнтові, представившись співробітниками організації та обманним шляхом дізнатися паролі від систем дистанційного банківського обслуговування і вивести гроші з рахунку клієнта.

У нашій країні проблема крадіжки та незаконного поширення персональних даних стоїть дуже гостро. У мережі Інтернет існує велика кількість ресурсів, на яких містяться крадені бази персональних даних, за допомогою яких, наприклад, за номером мобільного телефону, можна знайти дуже детальну інформацію по людині, включаючи його паспортні дані, адреси проживання, фотографії та багато іншого.

Розвиток інформаційних технологій і повсюдна інформатизація суспільства дають як позитивні, так і негативні результати. Збільшення кількості інформації та інформаційних потоків в суспільстві веде до вдосконалення багатьох процесів, розвитку і поліпшення взаємодії, але також породжує нові загрози й новий тип зловмисників, які оперують в рамках віртуальних даних.

Важливо розуміти, що сучасне суспільство у всіх своїх видах діяльності та секторах повсюдно і повсякденно використовує великі масиви даних, які обробляються, використовуються або зберігаються в різних системах. Тут варто зазначити, що інформацію можна визначити, як ресурс з високою цінністю, оскільки своєчасна і відповідна інформація може дати гігантську перевагу конкурентам або гравцям на ринку, будь то економічний сектор або якось вплинути на виробництво товарів і благ в будь-якому іншому. Таким чином інформація, як ресурс, має цінність, яку необхідно захищати. З цього випливає, що будь-які типи витоків інформації загрожують її власникам, часом, колосальними збитками.

Уявіть, що спам, що приходить вам на пошту, може бути причиною продажу ваших персональних даних третій особі або як в результаті крадіжки з компанії, де вони зберігалися. Але це найлегше, що може статися при витоку персональних даних. Недостатня захищеність інформаційних систем персональних даних може привести до крадіжки грошових коштів з рахунків, неправомірному використанню чужих кредитних рахунків, електронних облікових записів, підписів, електронних машин, отримання доступу до інших систем, іншим крадіжок і так далі. Все це доводить наскільки актуальна проблема інформаційної безпеки вже зараз і наскільки серйознішою вона стане в найближчому майбутньому.

При розробці системи інформаційної безпеки, необхідно озиратися не тільки на технічні фактори реальних проблем, а й на їх нормативно-правові

аспекти, які не менш важливі. Таким чином, регламент безпеки інформаційної системи персональних даних повинен містити наступні пункти:

- порядок доступу фахівців до роботи в програмних комплексах, що містять персональні дані;

- порядок організації системи розмежування доступу;

- порядок копіювання та зберігання інформації, що містить персональні дані;

- використання засобів інформаційної безпеки при обробці персональних даних.

1 ЗАГАЛЬНА АНАЛІЗ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДПРИЄМСТВІ

1.1. Характеристика персональних даних

Персональні дані підпадають під дію багатьох державних нормативів, основний з яких - Конституція України. У цьому документі пояснюється термін “персональні дані”, а також з чого складається це поняття. Виконання вимог цього нормативу - прямий обов’язок юридичних і приватних осіб.

До персональних даних (далі ПД) відносять відомості, що характеризують прямо або побічно суб’єкта - фізична особа. За таких даних можна найточніше встановити особистість конкретного громадянина.

Конституція України гарантує фізичним особам право на дотримання таємниці їхнього приватного життя, створює всі необхідні передумови для недоторканності та необхідного захисту. Власнику ПД належить все, з чого складається це поняття, у зв’язку з цим така інформація не повинна контролюватися третіми особами або урядовими органами [1].

Фізичні особи самостійно розпоряджаються своїми даними та вільні вирішувати - перешкодити їх поширенню або надати на вимогу. Держава надає певні гарантії та захист для отримання цієї можливості.

Носій ПД може дозволити операторам отримувати та здійснювати обробку його особистої інформації. Це дозволить на законних підставах виконувати певні дії з нею. Під час оформлення заяв на отримання позики, при оформленні на роботу, при проведенні анкетування фізична особа самостійно надає свою згоду, добровільно підписуючи угоду про дозвіл перевіряти його особисті дані.

Службові особи можуть скористатися доступом до певного обсягу особистої інформації, необхідної для виконання конкретних дій. У них немає

права на зберігання і застосування ПД після досягнення результату. У разі порушення такої вимоги оператор відповідає за їх навмисне розголошення.

У певних випадках використовується особлива вимога по роботі з ПД, якщо вони:

- необхідні для розв'язання питань сімейного або особистого характеру (у разі якщо поширення даних не призводить до ущемлення прав інших осіб);
- знаходяться в архівній документації;
- належать до даних, що становлять державну таємницю;
- повинні бути надані за судовим актом.

Різновиди ПД

Вони можуть класифікуватися за ступенем секретності, складності їх збору, можливості застосування третьою стороною. Їх поділяють на такі види:

- загальні;
- біометричні;
- спеціальні;
- знеособлені.

Загальні

До загальних відносять персональну інформацію, що становить базові дані про її носії: прізвище, ім'я, по батькові; місце реєстрації та проживання; інформацію з паспорта; відомості про наявне освіті; інформацію про місце роботи; відомості про отримувані доходи та ін.

Взяті окремо дані загального характеру можуть бути не всі занесені до інформації про людину, яка може вважатися персональною. Наприклад, в законі не міститься певних трактувань щодо того, чи можна вважати однією зі складових ПД номер телефону фізичної особи [1]. Як роз'яснюють в Кіберполіції України, ці дані не є інформацією, що дозволяє зробити точну ідентифікацію людини. Але при спільному використанні з прізвищем, ім'ям, даними про прописку він становить ПД.

Інформація про людину, яка є загальною, вказана в паспорті, її вносять у військовий квиток, в документ про освіту, а також в особисту картку співробітника підприємства, трудову книжку та інше. Щоб використовувати такі дані, не потрібно брати у співробітника письмовий дозвіл з метою їх отримати.

Досить того, щоб людина побічно, шляхом проставлення галочки у відповідному полі, підтвердив право на такі дії з боку одержувача цієї інформації в письмово складеній або онлайн - анкеті.

Отримати такі ПД дуже просто, а це часто призводить до проблем: починають розсилати нав'язливі рекламні пропозиції або, ще гірше, намагаються шантажувати, підробляти заявки на отримання позики та ін.

Від нерозголошення особисті дані кожного фізичної особи, які містять в собі певні різновиди секретних відомостей (про усиновлення, наявності захворювань і ін.), Захищаються законом № 383-VII України [8].

Біометричні

Є персональні дані, які характеризують носія по біологічному і фізіологічному принципу. До них відносять:

- дактилоскопічні;
- аналіз ДНК;
- групу крові;
- зріст, колір очей, вага та ін.

До біометричних персональних даних відносять інформацію, що отримується в результаті фотозапису за участю людини. Дані біометрії найбільш часто уживані під час проведення лікування, при оформленні на роботу в держструктури, при виготовленні закордонного паспорта і візових документів [16].

Спеціальні

До спеціальних ПД віднесені національна приналежність і раса, а також віросповідання, переконання філософського характеру, інформація про судимості, стан здоров'я, перевагах в сексуальній, інтимного життя. Ці відомості можна знайти в особистих справах, медичної документації тощо. Вони необхідні під час проведення політичних заходів, використовуються при вступі до лав збройних сил. Щоб треті особи могли отримати доступ і скористатися цими ПД, необхідно отримати дозвіл їх власника.

Знеособлені

До знеособлених даних відносять ПД, що мають загальну доступність. Їх можна знайти в адресних книгах, довідкової документації, в засобах масової інформації. Інформація, яка є загальнодоступною, може легко бути використана зацікавленими особами. Загальнодоступними є дані про матеріальне становище політичних діячів, представників влади, чиновників, що займають керівні пости.

Персональні дані - використання на підприємстві

Такі ПД повинні зберігатися належним чином і застосовуватися для того, щоб допомогти працівнику виконувати його обов'язки відповідно до його посадою і професією, просуватися по службовій драбині, підвищувати свою кваліфікацію та отримувати нові професійні знання. Також ПД використовуються з метою захисту співробітників і майна компанії [5].

Особиста інформація співробітника може містити тільки ті дані, які відносяться до його професійних якостей, особливостей, що дозволяє йому виконувати трудові обов'язки. За Конституцією України, особисте життя вважається недоторканною і конфіденційної, її частиною є ПД.

У Трудовому кодексі вузько визначено дане поняття. У ньому говориться, що ПД працівника є відомостями, необхідними керівництву підприємств для виконання ним своїх професійних обов'язків, ця інформація відноситься до конкретного працівника.

Обробка ПД

Метою, яку переслідує обробка і зберігання ПД на підприємстві, є необхідність правильно реалізувати робочу активність компанії. Обробка ПД необхідна для :

- фіксації факту прийняття співробітника на роботу;

- посвідчення підстав для просування по кар'єрних сходах;

- підтвердження підстав для виплати зарплати;

- здійснення контролю за виконанням виробничих завдань і робіт.

Працівникам компанії повинна бути доступна інформація про те, яким чином здійснюється зберігання та обробка їх особистих даних, тому роботодавець зобов'язаний ознайомити їх з даною інформацією. Підтвердженням того, що співробітники були повідомлені про це, є особистий підпис кожного з них [7].

Типи персональних даних на підприємстві

На підприємстві необхідно зібрати два типу ПД:

- необхідних для укладення трудового договору;

- запитуваних і формованих безпосередньо роботодавцем.

ПД, які зберігаються на підприємстві в особистих справах за кожним працівником, зазвичай містять дані:

- про сімейний статус і окремих членів родини (утриманці, діти, вікові дані, кількість, дані про стан здоров'я та ін.);

- копії документів по пенсійному державному страхуванню;

- про конкретного співробітника (паспортні дані, професія, кваліфікаційні характеристики та ін.).

Роботодавець повинен створити та затвердити внутрішній нормативний акт, який визначає порядок зберігання ПД у вигляді Положення про ПД або Інструкції. Дані нормативи повинні бути доведені до відома працівників, які

відповідальні за збір та обробку персональних даних. Вони повинні неухильно дотримуватися всіх вимог, викладені в таких документах.

При дотриманні всіх формальностей на підприємстві зі збору, зберігання і використання ПД вони будуть максимально захищеними.

Відповідальність за розголошення

Статтею 182 Кримінального кодексу України, передбачено захищати персональні дані фізичних осіб, передбачає виключно адміністративний вид відповідальності в разі розголошення ПД на підприємстві. Відповідно, якщо компанія не здатна надати своїм найманим працівникам повний захист особистих даних, роботодавець може бути покараний тільки штрафом. Дане покарання виражається незначними сумами [13].

Штраф, який повинен бути накладений на роботодавця при виявленні порушень такого характеру, може скласти в межах 2 - 5 тисяч гривень. Але це стосується одиничного порушення. Зазвичай при перевірках виявляють значну кількість такого роду проблем, відповідно, і суми штрафів при цьому ростуть.

Але фінансові витрати - це не основний наслідок неправильного використання і зберігання ПД. Такі факти позначаються на репутаційних показниках компанії. Якщо співробітники погоджуються на обробку персональних даних, вони повинні бути впевнені, що підприємство гарантує її правильне зберігання і використання.

Зловмисний витік даних дуже сильно перекликається із навмисним витоком та по своїй суті являється його частиною, за виключенням що, мета його здійснення є отримання будь - якої форми переваги.

Типова схема такого витоку представлена нижче(Рисунок 1.1).

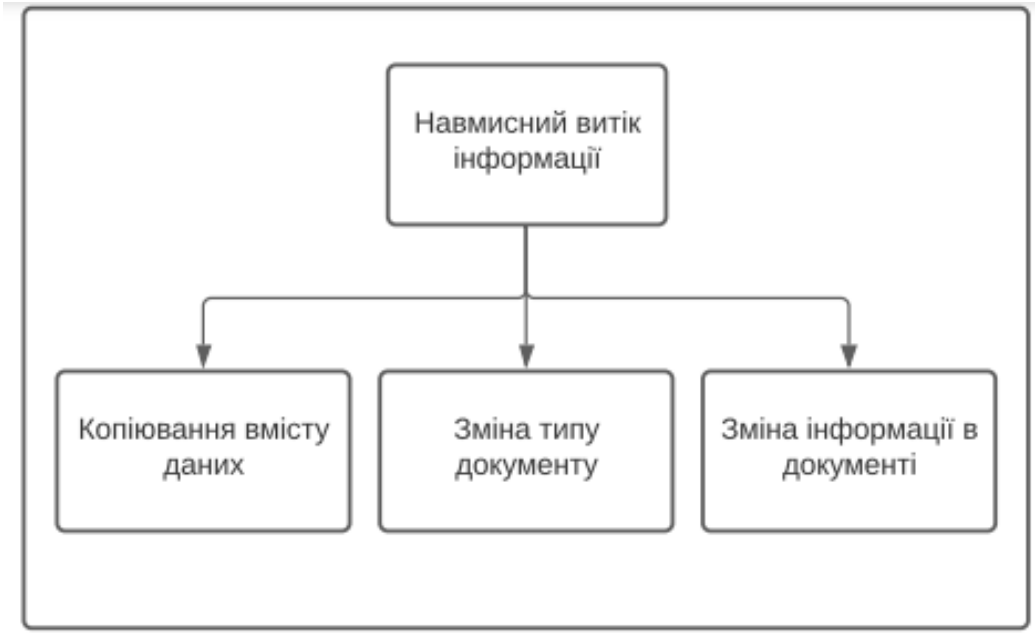


Рисунок 1.1 – Схема зловмисного витоку даних

1.2.Організація захисту персональних даних на підприємстві

Щоб захистити повний обсяг даних організації, потрібно знати свої дані: де вони знаходяться, чиї це дані та які дані вразливі.

Традиційні рішення для захисту даних часто будуються спеціально для того чи іншого типу зберігання даних: у гібридному середовищі може бути важко керувати даними, контролювати та захищати їх.

Точкові інструменти заблоковані, рідко пропонуючи повний огляд даних організації: вони можуть зосередитись на неструктурованих даних у конкретних попередніх середовищах, конкретних типах неструктурованих даних, що зберігаються в хмарі, або зосередитись виключно на неструктурованих даних - і організації не можуть будувати викласти повну картину даних, що поєднує розуміння та відбиття неструктурованих, на половину структурованих та структурованих даних для окремих ідентичностей, типів класифікації або аналізу на основі сутності.

Рішення щодо конфіденційності даних та безпеки повинні мати можливість охоплювати попередні, хмарні та гібридні середовища. Організації повинні мати можливість автоматично виявляти та ідентифікувати конфіденційні дані на своєму підприємстві - незалежно від того, де вони зберігаються [4].

Такі методи машинного навчання, як кластерний аналіз, є гнучким та масштабованим способом отримати уявлення про неструктуровані дані, автоматично аналізуючи та інвентаризуючи великі обсяги неструктурованих даних для виявлення конфіденційних та регульованих даних.

Інтелектуальне виявлення даних - це перший крок у захисті корпоративних даних: ви можете захистити лише те, що бачите.

Класифікуйте свої дані, щоб ефективно керувати політикою та застосуванням. Неструктуровані, на половину структуровані та структуровані дані слід класифікувати для кращого управління, захисту та обробки даних.

Визначення того, що являє собою особисту та конфіденційну інформацію - або різні типи регламентованої інформації – розширюється. Вона вже не базується виключно на регулярних виразах, а частіше на основі ідентичності.

Це означає можливість автоматичної ідентифікації та класифікації всіх типів конфіденційної інформації на основі змісту та структури даних - особиста інформація особиста інформація та конфіденційні дані - не обмежуючись певним класифікатором.

Організації повинні мати можливість автоматично класифікувати дані за особами, типами, категоріями, ознаками тощо: від імен до політичної діяльності до географічних даних; від регульованих даних, таких як медичні записи, до фінансових звітів до юридичних документів; від атрибутів безпеки, таких як паролі, до ключів продукту до зашифрованих приватних ключів.

Після того, як ви зможете ідентифікувати та виявити всі ваші дані, ви зможете застосовувати мітки, мітити типи даних та збагачувати їх додатковим контекстом для кращої автоматизації управління даними та захисту даних.

Дані без контексту небезпечні: важливо встановити та скласти зв'язки між даними, щоб не тільки зрозуміти, якими даними ви володієте, але і щоб ви могли впровадити політики для їх захисту. Кореляція будує контекст навколо наборів даних та взаємозв'язків, щоб організації могли краще зрозуміти, які конфіденційні дані у них є, де вони мешкають та як їх захистити.

Проводячи співвідношення, організації можуть виявити темні дані, які в іншому випадку є вразливими до компромісів, - і пов'язати ці темні дані з конкретними особами, сутностями або іншими наборами конфіденційних даних.

Застосування машинного навчання та розпізнавання нейронних сутностей (NER) розширює розуміння інтелекту даних: рішення щодо захисту даних повинні мати можливість автоматичної інтерпретації даних, щоб створити глибокі уявлення про дані [9].

Ключовим фактором будь-якого підходу до безпеки є виявлення, управління та зменшення ризику. Зараз CISO та групи безпеки перебувають під посиленим контролем з метою мінімізації ризику та захисту конфіденційних даних - починаючи з видимості та охоплення даних, що перебувають під загрозою.

Організаціям потрібно узгоджувати конфіденційність, щоб мінімізувати ризик, використовуючи передові дані та інформацію. Встановити політику щодо переміщення та дотримання даних, щоб відстежувати передачу даних, зловживання та порушення політики - з метою кращого впровадження політики безпеки та найкращих практик.

Статистика інформації про доступ забезпечує більшу видимість даних, що перебувають під загрозою. Глобальні групи доступу представляють одну з

найбільших вразливостей неструктурованих даних. Завдяки можливості ідентифікувати надмірно експоновані дані, організації можуть легко ідентифікувати джерела даних з високим ризиком та особливо вразливі записи, отримуючи пріоритетні уявлення про те, де зменшити ризик.

Моделювання ризиків може допомогти організаціям зрозуміти та порівняти ризик даних на основі чутливості даних, постійності, безпеки даних та доступу до додатків - і має бути налаштованим відповідно до галузі, типу даних та профілю компанії.

Для адекватного управління та зменшення ризику організаціям потрібно застосовувати підхід до захисту даних, орієнтований на конфіденційність, дотримуючись принципів розробки приватного життя, отримуючи на 360 ° видимість даних, що перебувають під загрозою, та керувати єдиною інвентаризацією конфіденційних даних по всій території. підприємство.

Порушення даних - це вже не якщо, а коли.

Найважливішим фактором є те, наскільки організації здатні реагувати на порушення: як пом’якшити наслідки, визначити вплив, повідомити постраждалих та спростити розслідування.

Організації можуть мінімізувати вплив порушення, маючи можливість швидко і точно визначити, які саме чиї дані були скомпрометовані.

Коли ви почнете з інтелектуального відкриття, класифікації наступного покоління та повної видимості ваших найбільш конфіденційних даних, ви зможете отримати більше від наявних та майбутніх інвестицій у безпеку, починаючи від застосування DLP та закінчуючи інтеграцією GRC.

Спростіть організацію та забезпечення безпеки, інтегрувавши свою політику безпеки з DRM, DLP, шифруванням, позначкою та іншими інструментами - все на основі базового розуміння того, що таке ваші конфіденційні дані, де вони мешкають і який тип політики безпеки слід застосовувати до конкретних категорій даних.

1.3 Існуючі системи захисту інформації

Розглянемо рекомендації для співробітників, для захисту даних на робочому місці. Якщо співробітник покидає робоче місце, знаходячись в центрі проєкт, що включає ділову конфіденційну інформацію, він має виконати низку запобіжних заходів мір захисту:

- захистити дані компанії від відвідувачів або інших осіб, які не мають права переглядати цю інформацію;

- заблокуйте комп'ютер;

- змініть налаштування, та встановіть надійний пароль для свого облікового запису;

- після зустрічі переглянути матеріали та виконати їх очищення;

- після друку, копіювання забрати свої документи одразу;

- зберігати конфіденційні документи у належних місцях;

Розглянемо метод, що вважається найпростіший метод контролю – сигнатури. Являти собою пошук у потоці даних певної послідовності символів, зазвичай представлена не словом, а довільним набором символів, наприклад є певною міткою. Якщо система налаштована тільки на одне слово, то результат її роботи — визначення 100 % збігу, тобто метод можна віднести до детерміністського [17].

Однак частіше пошук певної послідовності символів все ж таки застосовують при аналізі тексту. В переважній більшості випадків сигнатурні системи налаштовані на пошук декількох слів і частоту зустрічальності термінів. До переваг цього методу можна віднести простоту поповнення словника заборонених термінів і очевидність принципу роботи, а також те, що це найбільш надійний спосіб, якщо необхідно знайти відповідність слова або виразу на 100 %.

Недоліки стають очевидними після початку промислового використання такої технології при визначенні витоків і налаштуванні правил фільтрації. Більшість виробників DLP-систем працюють для західних ринків, а англійська мова дуже ‘сигнатурна’ – форми слів найчастіше утворюються за допомогою прийменників без зміни самого слова.

Реальне застосування цього методу вимагає наявності лінгвіста або команди лінгвістів як на етапі впровадження, так і в процесі експлуатації та оновлення бази [17].

Безсумнівним недоліком є і те, що «сигнатури» нестійкі до примітивного кодування, наприклад, заміною символів на схожі за зображенням.

Принцип роботи DG досить проста і часто цим і приваблює: DLP/IPC-системі передається якийсь стандартний документ-шаблон, з нього створюється «цифровий відбиток» і записується в базу даних DF.

Далі в правилах змістовної фільтрації настроюється процентна відповідність шаблону з бази. Наприклад, якщо налаштувати 75 % відповідності «цифровому відбитку» договору постачання, то при змістовній фільтрації DLP виявить практично всі договори цієї форми.

Іноді, до цієї технології відносять і системи на зразок «анти плагіат», однак остання працює тільки з текстовою інформацією, водночас як технологія «цифрових відбитків», у залежності від реалізації, може працювати й різним медійним контентом і застосовуватися для захисту авторських прав і перешкоди випадкового або навмисного порушення законів і нормативів інформаційної безпеки.

Великі компанії, в яких з’являється до десятка тисяч нових і оновлених документів кожен робочий день тільки на серверних сховищах часто просто не в змозі відстежувати все це в режимі реального часу, не кажучи вже про персональні комп’ютери та ноутбуки.

Суть цього методу полягає у призначенні спеціальних «міток» всередині файлів, що містять конфіденційну інформацію. З одного боку, такий метод дає стабільні та максимально точні відомості для DLP-системи, з іншого – потрібно досить сильні зміни в інфраструктурі мережі. У лідерів DLP/IPC-ринку реалізація даного методу не зустрічається, тому розглядати її докладно не має особливого сенсу.

Можна лише зауважити, що, попри явну перевагу «міток» – якість детектування, є багато суттєвих недоліків. Від необхідності значної перебудови інфраструктури всередині мережі до введення безлічі нових правил і форматів файлів для користувачів. Насправді застосування такої технології перетворюється у впровадження спрощеної системи документообігу.

Пошук за регулярними виразами «масками» є також давно відомим способом детектування необхідного вмісту, однак в DLP він став застосовуватися відносно нещодавно. Часто цей метод називають «текстовими ідентифікаторами». Регулярні вирази дозволяють знаходити збіги за формою даних, у ньому не можна точно зазначити точне значення даних, на відміну від «сигнатур».

До переваг технології регулярних виразів у першу чергу варто віднести те, що вони дозволяють знаходити специфічний для кожної організації тип наповнення, починаючи від кредитних карток і закінчуючи назвами схем обладнання, специфічних для кожної компанії.

Крім того, форми основних конфіденційних даних змінюються вкрай рідко, тому їх підтримка практично не вимагатиме часових ресурсів.

До недоліків регулярних виразів можна віднести їх обмежену сферу застосування в рамках DLP/IPC-систем, так як знайти за допомогою них можна тільки конфіденційну інформацію. Регулярні вирази не можуть

застосовуватися незалежно від інших технологій, однак можуть ефективно доповнювати їх можливості.

Лінгвістичні методи. Найбільш поширеним на сьогодні методом аналізу в DLP/IPC-системах є лінгвістичний аналіз тексту. Він настільки популярний, що часто саме він у просторіччі іменується «тематичною фільтрацією», тобто несе на собі характеристику всього класу методів аналізу вмісту. Є технології, які використовують лише «стоп-вирази», що вводять тільки на рівні коріння, а сама система вже становить повний словник; є що базуються на розставленні ваг на терміни, що найчастіше зустрічаються в тексті.

Є у лінгвістичних методах і свої відбитки, що базуються на статистиці; наприклад, береться документ, рахується п’ятдесят найбільш уживаних слів, потім вибирається з 10 найуживаніших з них у кожному абзаці. Такий «словник» є практично унікальною характеристикою тексту і дозволяє знаходити в «клони» значущі цитати [14].

До заслуг лінгвістичних методів у DLP можна віднести те, що в морфології та інших лінгвістичних методах високий ступінь ефективності, у порівнянні з сигнатурами, при набагато менших трудовитратах на впровадження і підтримку. У випадку з використанням лінгвістичних методів детектування нема потреби відстежувати появу нових документів і направляти їх на аналіз у IPC-систему, так як ефективність лінгвістичних методів визначення конфіденційної інформації не залежить від кількості конфіденційних документів, частоти їх появи та продуктивності системи фільтрації вмісту.

Недоліки лінгвістичних методів також досить очевидні, перший з них – залежність від мови – якщо організація представлена в декількох країнах, бази конфіденційних слів і виразів доведеться створювати окремо для кожної мови та країни, з огляду на всю специфіку.

Ручна перевірка конфіденційної інформації іноді називається «Карантин». Будь-яка інформація, яка потрапляє під правила ручної перевірки, наприклад, у ній зустрічається слово «ключ», потрапляє у консоль фахівця інформаційної безпеки. Він по черзі вручну переглядає цю інформацію та приймає рішення про пропуск, блокування або затримку даних. Коли дані блокуються або затримуються, відправнику надсилається відповідне повідомлення. Безперечною перевагою такого методу можна вважати найбільшу ефективність [9].

Однак, такий метод у реальному бізнесі можна застосовувати лише для обмеженого обсягу даних, тому що потрібно велика кількість людських ресурсів, так як для якісного аналізу всієї інформації, що виходить за межі компанії, кількість співробітників інформаційної безпеки має приблизно збігатися з кількістю інших офісних співробітників. Реальне застосування для такого методу – аналіз даних обраних співробітників, де потрібна більш тонка робота, ніж автоматичний пошук за шаблонами, «цифрових відбитків» або збігів зі словами з бази.

1.4.Висновки

Для кваліфікаційної роботи було зібрано надзвичайно багато інформації та виявлено взаємозалежність між новими розробками та розповсюдженням інформаційної небезпеки. Враховуючи таку ситуацію на цей час суб’єкти зі злоякісними цілями будуть і надалі намагатися отримати доступ до конфіденційних даних, що буде породжувати нові технології злому та захисту даних.

2 ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ТОВ ЕСКО ЕКО ІДЕЯ

2.1. Опис обраної мови програмування C#

Для розроблювальної системи «Організації захисту персональних даних в підприємстві ТОВ < ЕСКО> < ЕКО-ІДЕЯ> мною було відібрано мову програмування C# в клієнтському лаунчері Visual Studio та SQL Server .

2.2 Підходи до аналізу захисту

Система захисту інформації - це комплекс організаційних і технічних заходів, спрямованих на забезпечення інформаційної безпеки підприємства. Головним об'єктом захисту є дані, які обробляються в автоматизованій системі управління (АСУ) і залучений при виконанні бізнес-процесів[18].

Основні загрози для інформаційної безпеки будь - якої компанії пов'язані з крадіжкою даних (наприклад, промислове шпигунство), використанням неперевіреної програмного забезпечення (наприклад, що містить віруси), хакерськими атаками, отриманням спаму (також може містити віруси), халатністю співробітників. Рідше втрата даних викликана такими причинами, як збій в роботі апаратно-програмного забезпечення або крадіжка обладнання. В результаті компанії зазнають значних втрат.

Процес створення системи захисту інформації можна розділити на три етапи:

- формування політики підприємства в області інформаційної безпеки;
- вибір і впровадження технічних і програмних засобів захисту;
- розробка і проведення ряду організаційних заходів.

При цьому слід враховувати державні нормативні документи та стандарти, які регулюють питання інформаційної безпеки на підприємствах.

Основні методи:

Метод висунення гіпотез полягає в процедурі відділення відомого від невідомого і вирахуванні в невідомому окремих, найбільш важливих елементів і фактів (подій).

Метод інтуїції полягає в використанні аналітиком своєї здатності до безпосереднього осягнення істини (досягненню необхідного результату) без попереднього логічного міркування. Багато в чому цей метод ґрунтується на особистому досвіді аналітика.

Метод спостереження полягає в безпосередньому дослідженні (Обстеженні) конкретного об'єкта (джерела інформації, події, дії, факту), в самостійному описі аналітиком будь-яких фактів (подій, процесів), а також їх логічних зв'язків протягом певного часу.

Мета методу порівняння полягає в більш глибокому вивченні процесів (подій), що відбуваються на підприємстві та мають відношення до питань захисту охороняється інформації. порівнюються різні фактори, що зумовлюють причини та обставини, що призводять до витоку конфіденційної інформації або до виникнення передумов до її витоку. При використанні методу порівняння в обов'язковому порядку дотримуються наступні основні умови: порівнювані об'єкти (Дії, явища, події) повинні бути порівнянні за своїми якісними особливостями; порівняння повинно визначити не тільки елементи подібності, а й елементи відмінності між досліджуваними об'єктами.

2.3 Технічне завдання на розроблювану систему

Назва розроблюваної системи: Організація захисту персональних даних в підприємстві ТОВ <ЕСКО ><ЕКО-ІДЕЯ>.

Метою даної розроблюваної системи є організація мір по захисту від витоків персональних даних в інформаційному середовищі підприємства.

Додатковою метою створення розроблюваної системи є впровадження власної розробки яка може задовольнити потреби захисту від витоків персональних даних.

Система призначена для моніторингу та запобігання втрати персональних даних з підприємства, що містять конфіденційну інформацію.

Сферою застосування є забезпечення захисту від витоків даних пов’язаних із несанкціонованим доступом.

2.4 Загальна характеристика розроблюваної системи

В рамках проєкт необхідно реалізувати додатковий захист основного сервера серед функцій якого будуть:

- централізоване управління доступом до інформації;
- користувачі отримають доступ тільки до тих даних, які їм потрібні;
- доступ до файлів можна гнучко налаштувати для різних користувачів;
- контроль. На сервері терміналів не вийде гратися в розважальні ігри - всі співробітники будуть зайняті роботою;
- обслуговування файлового сховища;
- сховище баз даних для структуризації та швидкого доступу до корпоративної інформації;

2.3Висновки

У ході аналізу теперішніх мов програмування на сьогоднішній час мною було обрано C# у видані microsoft, тому що мова підтримує надзвичайно багато функцій та працює стабільно.

3 ПРОЕКТУВАННЯ СИСТЕМИ БЕЗПЕКИ

3.1 Система захисту персональних даних

3.1.1 Типова архітектура

Для розробки системи необхідно зрозуміти хто такий порушник та як з ним боротися. Нижче наведено рисунок 3.1 з типовим на сьогоднішній час порушником в системі.

Рисунок 3.1 – Типова модель порушника в системі

З малюнку ми бачимо, що порушник може бути будь - якого рівня, з випадковим технічним забезпеченням та своїми мотивами. В залежності від рівня кваліфікації порушник має свої мотиви. Порушник початківець який сидить скоріше за все за настільним офісним ПК навряд чи зможе зробити багато шкоди, але ігрові дії з цього боку все - таки можуть перерости в збиткові наслідки для компанії та самого порушника у вигляді витоку даних компанії та витоку персональних даних самого порушника.

Якщо ж говорити про порушника середнього рівня, то тут все стає більш серйозно. Такий порушник вже може шантажувати компанію на яку працює, то будь - який негативний вплив компанії на самого порушника будь то догана чи не виплата за працю. Як правило такий порушник має обладнання достатньо високого рівня, що дозволяє йому поводитися більш впевнено.

Але є і куди гірші порушники. Можна сказати, що це вже є хакер порушник. Такий тип порушників інформаційної безпеки діє вже ціле направлено та частіше за все працює за своєю схемою. Зазвичай такого хакера наймають компанії конкуренти для підриву з середини. Серед основних цілей даного хакера це саботаж та направлений витік даних зі стандартною метою її продажу. Як правило технічне забезпечення такого порушника буде за останнім словом техніки.

Щоб зрозуміти на якому місці знаходиться порушник в системі підприємства, необхідно звернути увагу на рисунок 3.2.

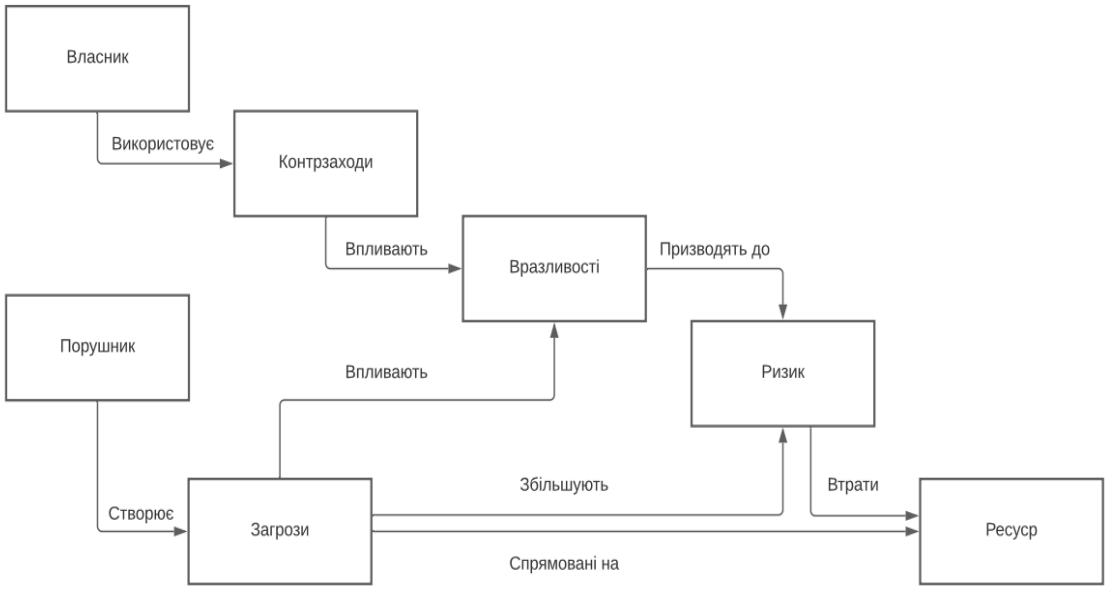


Рисунок 3.2 – Типова модель загроз системі

Коротко про малюнок:

- власник – це безпосередньо особа, яка стоїть вище всіх в ієрархії підприємства;

- порушник – це будь - яка особа що порушує будь - які правила;

- загрози – сукупність факторів, які представляють небезпеку;

- контрзаходи – дії спрямовані на збільшення захисту;

- вразливості – дії які можуть створити шкоду для підприємства;

- ризик – дії які можуть призвести до втрати даних або навпаки до їх збереження;

- ресурс – дані самого підприємства;

З рисунка ми бачимо, що порушник(як і з попереднього пункту) створює загрози, як самому собі, так і підприємству, які спрямовані на ресурси підприємства, що своєю чергою збільшує ризики втрати даних.

Тим часом власник же буде використовувати такі контрзаходи, які будуть впливати на вразливості негативно, що своєю чергою будуть

призводити до зменшення ризиків, що своєю чергою і значно зменшить ризик втрати персональних даних підприємства.

Серед основних контрзаходів існує:

- зовнішній захист

- внутрішній захист

До зовнішнього захисту можна віднести захист каналів та захист периметру. До внутрішнього захисту ОС, захист ПЗ та захист серверу підприємства.

Захист каналів. Організація захисту каналів мережі здійснюється за допомогою оптоволоконного кабелю. Його кварцовий сердечник дозволяє передавати дані у вигляді світлових сигналів, в які інформація конвертується за допомогою спеціального обладнання.

Це забезпечує високу швидкість проходження сигналу (до 100 Гбіт/с) і нечутливість виділеного каналу до впливу джерел електромагнітного випромінювання, інших несприятливих чинників.

Захист периметру. Класичний принцип забезпечення безпеки можна сформулювати приблизно так: максимально захистити користувачів від небезпек, що виходять ззовні. Що ж, небезпек ззовні більш ніж достатньо:

- комп’ютерні віруси які множаться;

- на місце одиноких вірусів приходять згуртовані банди;

- копійчаний прибуток поступається місцем тисячам доларів за розсилання небажаних поштових відправлень (спаму) і мільйонам доларів, вкрадених з рахунків користувачів;

Некомерційні віруси остаточно пішли в минуле в кінці 2007 року, і сьогодні вірус - це шкідлива програма, спрямована головним чином на отримання прибутку. Крім вірусів, існує безліч інших небезпек, що загрожують неприємними наслідками для організацій, - взяти хоча б DDoS-атаки, здатні повністю зупинити бізнес компанії на кілька днів.

Безумовно, захист кінцевих користувачів - це важливо. Але, як вже говорилося, повноцінна і надійний захист даних компанії можлива тільки при розумному підході до організації безпеки периметра мережі. Розв'язання цієї проблеми неможливе без використання найбільш безпечного і захищеного програмного забезпечення в серверній частині мережі.

В першу чергу від набігів ворогів страждає, звичайно, між мережевий екран: саме через нього проходить весь трафік компанії, саме йому доводиться справлятися зі шкідливими програмами та атаками ззовні.

Захист ОС. Під захистом ОС мається на увазі всі засоби та механізми захисту даних, що працюють в ОС. Під безпекою ОС розуміється такий стан ОС, при якому неможливо випадкове або навмисне порушення функціонування ОС, а також порушення безпеки знаходяться під управлінням ОС ресурсів системи.

Основною проблемою забезпечення безпеки ОС є проблема створення механізмів для контролю доступу до системних ресурсів. Забезпечення безпеки даних для роботи з ресурсами системи за допомогою кластеризації спеціальних програм операційної системи. Безперервних інструментів моніторингу, ведення реєстру для запису відомостей про всі події в системі.

Для захисту ОС може бути застосована сигналізація про несанкціонований доступ, використовується при виявленні порушення безпеки даних або спроби порушення.

Основні способи захисту несанкціонованого доступу до інформації - аутентифікація, авторизація (визначення прав доступу суб'єкта конфіденційної інформації), а також шифрування інформації. Контроль доступу до даних. При створенні механізмів контролю доступу необхідний в першу чергу для визначення наборів предметів і об'єктів доступу. Це можуть бути, наприклад, користувач, завдання процесів і т.д.

Логічний контроль доступу є основним механізмом багатокористувацьких систем, призначених для забезпечення конфіденційності та цілісності об’єктів і, до певної міри, їх наявність (щодо заборони надання послуг несанкціонованими користувачами).

Захист ПЗ. Розробники програмного забезпечення, які створюють платні продукти, навряд чи хочуть витратити кілька років свого життя на програму, яку тут же зламають і стануть використовувати безплатно. На сьогодні є багато різних рішень для ліцензування і захисту ПЗ. Один з найбільш надійних методів, який поєднує в собі переваги всіх інших стратегій. За ліцензування відповідає електронний USB-ключ, якому не потрібне підключення до мережі. Ціна кожного ключа для розробника низька, немає періодичних додаткових витрат. Реалізувати можна як за допомогою API, так і за допомогою програмної оболонки.

Перевагою такого методу є те, що ліцензію можна прибрати за межі операційної системи, ключ зберігається поза ПК. Ключ або дуже складно, або взагалі неможливо скопіювати. ПО, яке захищене за допомогою апаратного ключа, може використовуватися на тих системах, де немає підключення до мережі.

Це, наприклад, урядові об’єкти або промисловість. Ще один плюс в тому, що електронному ключу не потрібні різні рішення для різних програмних середовищ, а можливості ліцензування дуже гнучкі.

Рішення на основі апаратного ключа можна розгорнути буквально за хвилини, вони підтримуються практично будь-якими версіями операційних систем.

Захист серверу. Безпека комп’ютерів в організації дуже важлива, оскільки саме їх співробітники використовують для доступу до конфіденційної інформації. Якщо в налаштуваннях захисту ПК або сервера

при цьому є вразливість, то їй може скористатися як зовнішній зловмисник (хакер), так і інший недбайливий співробітник (інсайдер).

Це можуть бути й віруси, які пробиваються через проломи в захисті, так і майже “нешкідливі” програми - Майнер, що витрачають ресурси комп'ютерів організації на діяльність, вигідну зловмисникам.

Для захисту всіх цих загроз є цілий комплекс заходів, які дозволяють зміцнити захист апаратних засобів в інфраструктурі компанії (простіше кажучи комп'ютерів і серверів):

- регулярний аудит безпеки;
- правильні налаштування комп'ютерів і серверів, істотно ускладнюють злом або роблять його неможливим;
- установка засобів захисту;
- правильна структура мережі та підключення до серверів компанії.

Виходячи з вище проведеного аналізу даних я вирішив розробити власну систему захисту персональних даних на основі вже наявних даних та впровадженням своєї розробки вже в присутню систему захисту ЛОЗА – 2.

3.2 Опис функціонування системи

Згідно зі сформованим завданням, потрібно описати моделі потоків даних та схему роботи розроблюваної системи. Разом із цим потрібно описати інструменти підтримки та адміністрування даної системи.

Розробка системи захисту від витоків даних буде виконуватися згідно із клієнт-серверною архітектурою (рисунок 3.3). Дана архітектура передбачає розподілення функцій системи між провайдерами послуг та їх клієнтами. Фактично реалізацією провайдера та клієнта розроблюваної системи може бути програмне забезпечення. Класично провайдера послуг називають сервер.

Основною формою взаємодії клієнта та сервера є надсилання запитів через мережеве середовище зв’язку.

Клієнт – це додаток на робочій станції користувача, який надсилає запити на сервер і на основі відповідей серверу виконує певні інструкції.

Сервер – додаток на спеціалізованій робочій станції, яка налаштована для отримання запитів від багатьох клієнтів та обробки їх згідно з власної логіки роботи та надсилання відповіді на основі результатів обробки.

Рисунок 3.3

Адміністрування над системою буде здійснюватися за допомогою наступної панелі:

- панель налаштування.
- вихід.
- робоча зона.

Панель налаштування буде містити в собі такі пункти:

- зміна мови.
- налаштування інтерфейсу.
- посібник користувача.

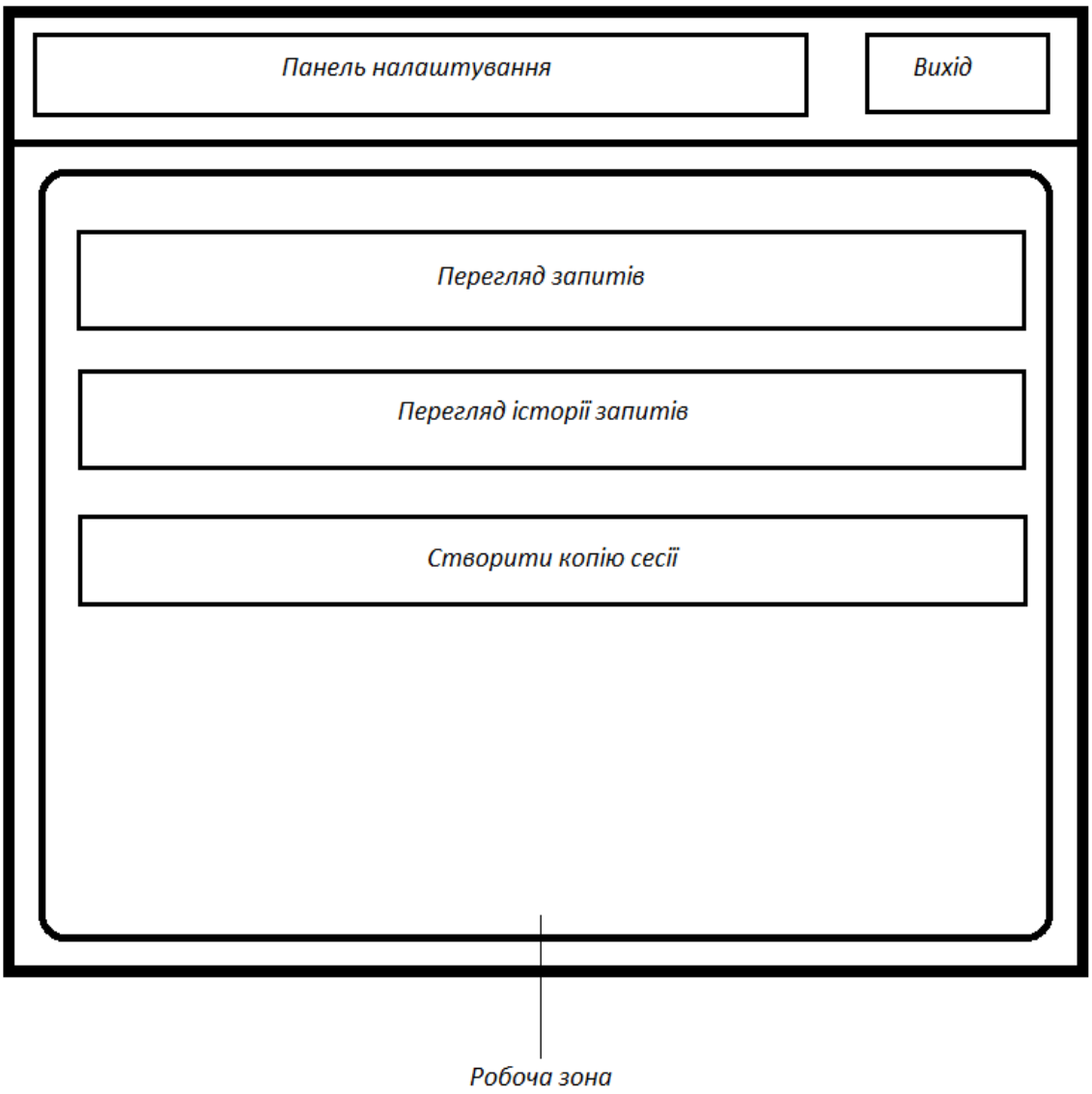


Рисунок 3.4 - Модель інтерфейсу керування системою

Робоча зона має наступні пункти:

- перегляд запитів
- перегляд історії запитів
- створити копію сесії

При виборі пункту перегляд запитів, буде можливість в реальному часі переглянути хто робить запити до сервера, звідки це відбувається, для якої цілі.

При виборі пункту перегляд історії, буде можливість переглянути історію переглядів, історію завантажень, історію форм запитів, історію пошукових запитів.

В пункті створити копію сесії в робочій зоні буде можливість створити копію всіх записів та історії запитів з можливістю її завантаження.

3.3 Розробка структурної схеми системи

Для організації системи захисту персональних даних пропонується вдосконалити системи захисту ЛОЗА – 2. Система впроваджується в середовище та здійснює відстежування потоків інформації пов’язаних із несанкціонованим доступом до конфіденційної інформації.

Серед основних переваг це:

- дозволяє захистити дані на стаціонарних носіях;
- дозволяє надійно захистити документи зв’язані з Microsoft office;
- містить в собі журнал подій;
- в стандартній конфігурації для входу в систему дозволяє ввести логін та пароль;

Типова архітектура системи захисту наведена в рисунку 3.4

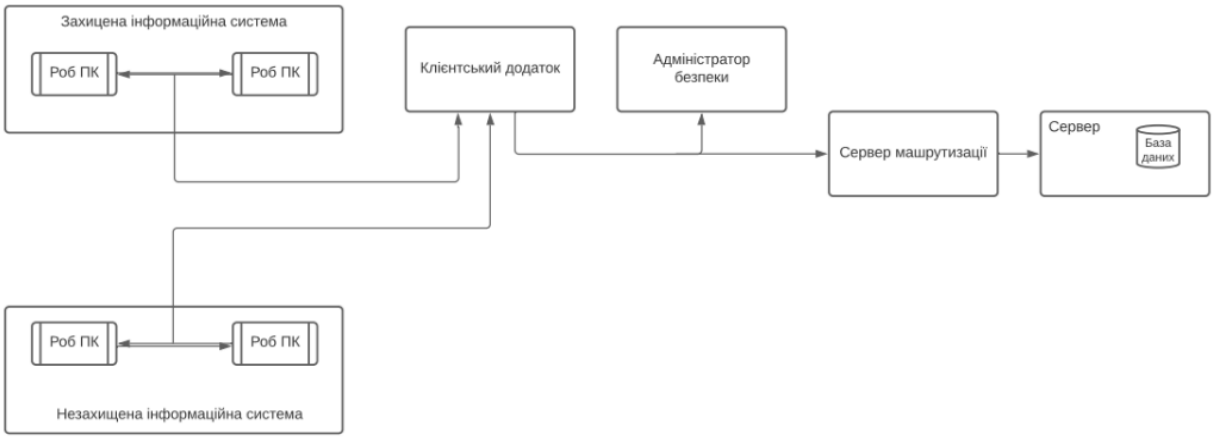


Рисунок 3.5 – Архітектура системи захисту

Програма не погана, але для реалізації моєї системи захисту не вистачає деяких покращень, а саме:

- захист даної програми не погани для домашніх ПК, але не для підприємства;
- на основі наявної програми впровадити систему управління, яка буде містити в собі нові компоненти, які позитивно вплинуть на стійкість до захисту;
- необхідно зробити зв’язок між співробітниками, сервером та адміністратором безпеки, тому що на цю мить адміністратор безпеки отримує інформацію про запити до сервера з великою затримкою.

Виглядати це має так як наведено в рисунку 3.6

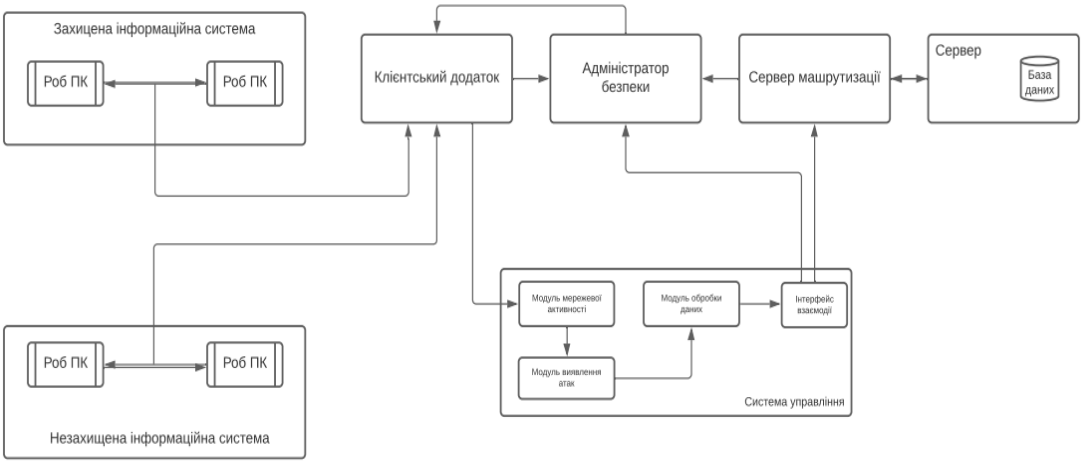


Рисунок 3.6 - Модифікована архітектура системи захисту даних

Серед компонентів архітектури є:

1) БД – база даних конфіденційної інформації, а також дані про користувачів системи, яка мітиться на сервері.

2) Сервер маршрутизації – сервер, який буде направляти на ту інформацію до якої був зроблений безпосередній запит і нікуди більше.

3) Адміністратор безпеки – людина, яка буде здійснювати додатковий захист конфіденційної інформації, прийняті важливих рішень, усунені загроз та їх блокуванні.

4) Система управління – служить бар'єром між клієнтським додатком та БД.

Система управління містить в собі:

1) Інтерфейс взаємодії – служить як інтерфейс взаємодії між сервером та клієнтським додатком.

2) Модуль обробки – необхідний для прийняття запитів до доступу даних, їх обробки та пошуку в БД.

3) Модуль виявлення атак - необхідний для моніторингу системи, збору мережевих даних та у разі виявлення порушника заблокувати його та сповістити про це адміністратора безпеки.

4) Модуль мережевої активності – мета модуля полягає в зборі даних мережевої активності та у разі виявлення порушника збору даних про нього.

5) Клієнтський додаток – необхідний для зв’язку між інформаційними ресурсами(робочими станціями) та сервером.

3.5 Висновки

В ході проєктної розробки було створено структуру майбутньої системи захисту персональних даних, сформоване технічне завдання на розроблювану схему. Для забезпечення ефективної розробки захисту персональних даних необхідно в структурну схему системи ввести модулі обробки, виявлення атак та модуль мережевої активності.

На стадії розробки виявлено проблеми пов’язані з передачею даних. Проблему було запропоновано вирішити шляхом модифікації архітектури розроблюваної системи.

4 РЕАЛІЗАЦІЯ РОБОТИ

4.1 Розробка блок-схем і опис алгоритмів функціонування системи

На основі описаного в 3 розділі технічного завдання та розробленої архітектури майбутньої системи захисту персональних даних приступаємо до розробки та реалізації алгоритмів функціонування системи.

Розглянемо алгоритм, який зображений на рисунку 4.1, роботи компонента мережевої активності клієнтів системи захисту персональних даних до сервера. Початковим етапом роботи системи управління є її розгортання. Процес розгортання відбувається при запуску серверу і відбувається один раз.

Модуль мережевої активності починає свою роботу з моніторингу запитів до сервера з БД. У разі якщо активності немає – система продовжує моніторинг активності запитів.

Якщо все ж таки є активність проводиться збір даних. В першу чергу проводиться збір даних чи вважається це атакою. Якщо ж ні, система збере дані про того хто і звідки зробив запит та запише це в журнал подій, повідомить про це адміністратора безпеки та повернеться до початку, а саме до моніторингу.

У разі якщо атака підтверджується збираються наступні дані:

- дані про порушника;
- дані про його дії;
- мета цих дій;

Коли дані зібрані, модуль буде намагатися заблокувати загрозу одночасно з цим сповістивши адміністратора безпеки.

Рисунок 4.1 – Алгоритм роботи модуля мережевої активності

Переходимо до алгоритму роботи модуля виявлення атак (рисунок 4.2). Модуль виявлення атак зв’язаний з модулем мережевої активності та починає свою роботу з моніторингу систем та приймання даних з попереднього модуля, обробляє їх та зберігає, як резервну копію. Далі на основі даних з попереднього модуля система визначає чи це порушник. Якщо ж ні, то система повернеться до початкової точки, моніторингу.

У разі підтвердження порушника модуль використовує попередні дані про порушника, які зібрав модуль мережевої активності та формує ознаки загрози. Після цього модуль класифікує загрозу за її ознаками для того аби було чітко зрозуміло з чим потрібно працювати.

Наступним етапом відбувається формування сигнатури атаки для того аби з’ясувати яким вірусом намагаються зломати систему. Коли все відомо приймається рішення про блокування загрози та сповіщення адміністратора безпеки про інцидент. Сповіщення про заблокування загрози надходять напряму до адміністратора безпеки

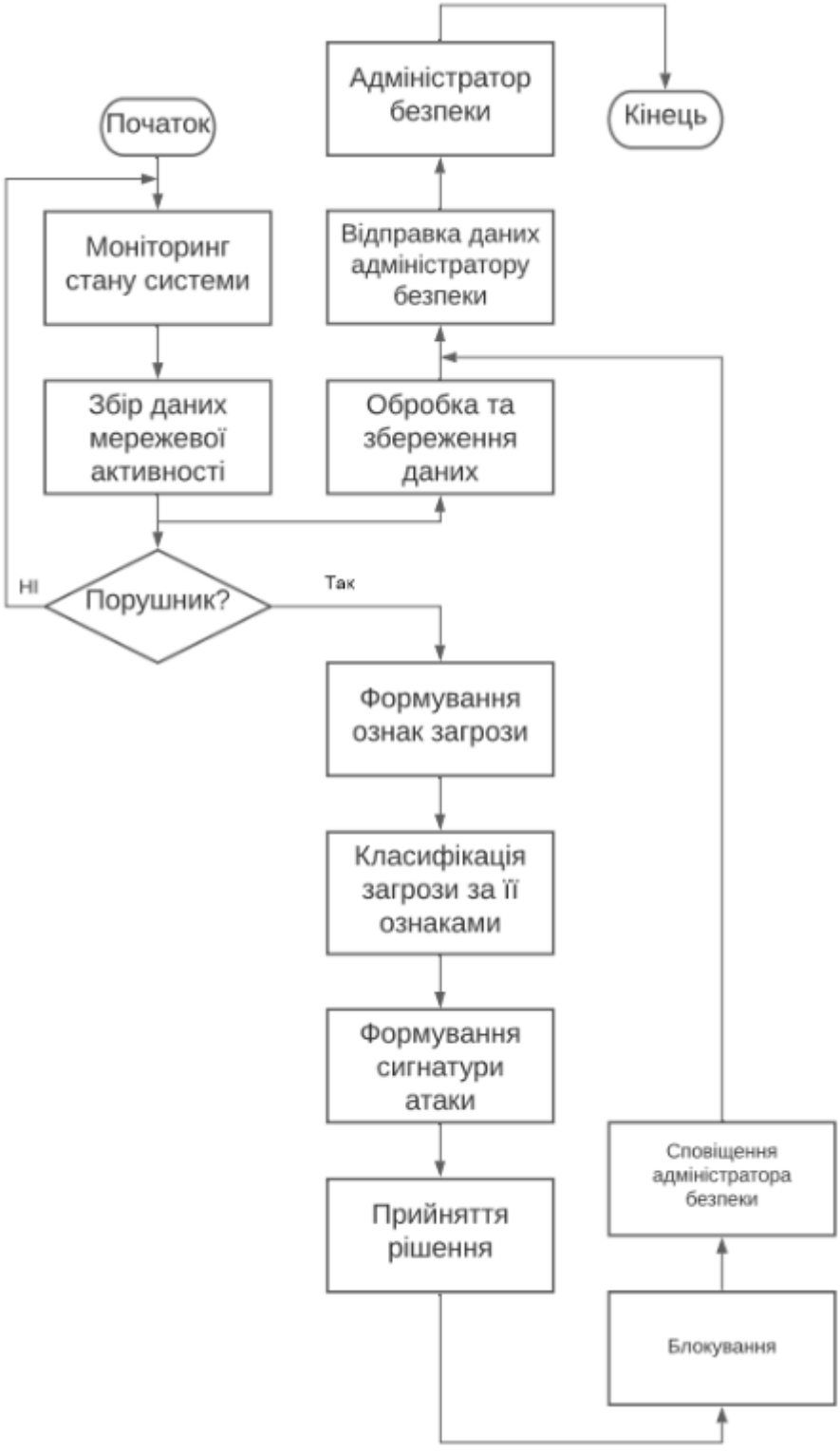


Рисунок 4.2 - Алгоритм роботи модуля виявлення атак

Модуль обробки даних необхідний для того, щоб запити, які надходять від співробітників потрапили до сервера маршрутизації в цілісності. Модуль приймає запит після двох попередніх модулів, які служать для третього як фаєрвол. На початку модуль приймає запит та обробляє його. Після цього модуль створює для клієнта запит на доступ до даних, але вже до сервера маршрутизації. Одночасно з цим відбувається обробка даних та їх пошук в БД.

Якщо дані знайдено, то запит клієнта приймає сервер маршрутизації який направляє співробітника туди куди робився запит і нікуди більше. Простіше кажучи у співробітника буде доступ тільки й тільки до тих даних до яких був початково здійснений запит.Одночасно з цим модуль збирає з попередніх модулів журнал подій, обробляє його та надсилає адміністратору безпеки.

У разі коли дані не знайдено клієнтський додаток повідомляє про невірно введений запит та надає можливість повторного підключення.

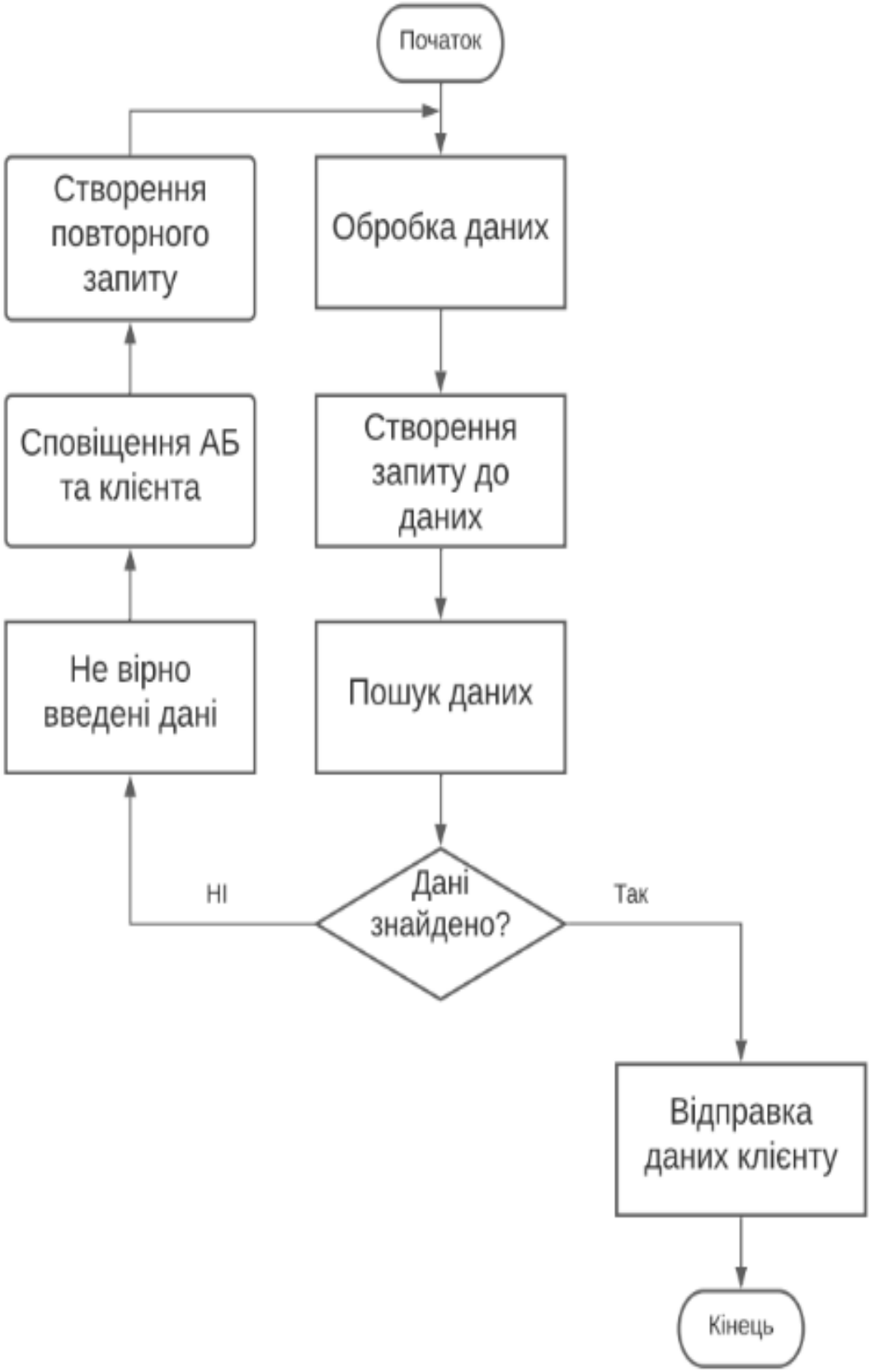


Рисунок 4.3 - Алгоритм роботи модуля обробки

4.2 Тестування системи

Для тестування системи було створено тестове середовище де було встановлено клієнт системи захисту персональних даних. Сервером виступала віртуальна машина під керування Linux.

Додатки емалювання діяльності користувача мали спільне сховище із документами, які використовувалися для операцій копіювання/переміщення файлів.

На рисунку 4.4 зображено графік кількості запитів і кількість витоків які було дійсно скоєно.

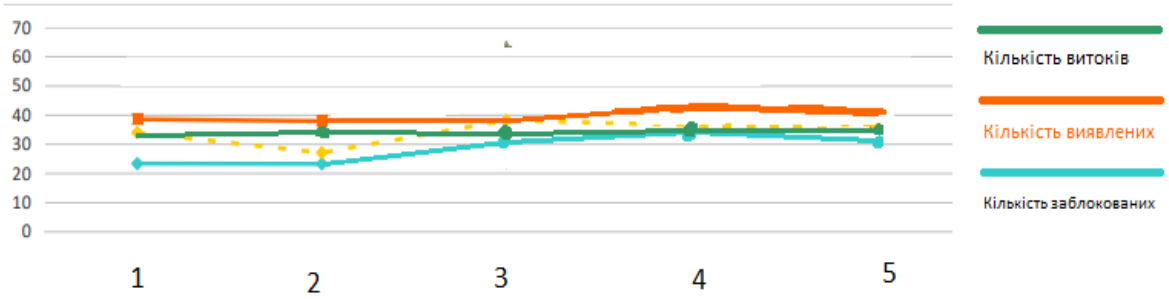


Рисунок 4.4 – Графік виявлених та заблокованих витоків

Як видно з рисунку 4.4 кількість успішно заблокованих витоків доволі не погана. на ефективність роботи вливає що тестування відбувається на одній реальній машині. Дане тестування дозволило виявити проблеми даної архітектури.

4.3 Впровадження системи в промислову експлуатацію

Система була реалізована на вже наявній системі ЛОЗА – 2. Завдяки запасу потужності даного програмного продукту я зміг впровадити свої покращення в систему без сповільнення процесу праці.

Підтримка та адміністрування системи здійснюється за допомогою інтерфейсу описаного в третьому розділі. Оновлення системи потрібно робити в разі зміни функціоналу системи захисту.

4.4 Висновки

У ході проектування та реалізації власної системи захисту персональних даних на підприємстві було розроблено систему, яка доволі успішно могла виявляти та блокувати витоки даних на підприємстві. Необхідно оптимізувати роботу системи для того щоб вона працювала швидше та ще ефективніше.

ВИСНОВКИ

На етапі обстеження була розглянута загальна характеристика об'єкта автоматизації, його організаційна структура та організація роботи. На основі аналізу сформовані і обґрунтовані вимоги до роботи системи і до її окремих компонентів: програмного, інформаційного, технічного.

На стадії проектування розроблена загальна структура інформаційної системи в цілому. Визначено основні проектні рішення, що стало підставою для розробки, налагодження програмної частини і для конструювання експлуатаційної документації.

Створення та впровадження системи захисту персональних даних на прикладі ТОВ <ЕСКО ><ЕКО-ІДЕЯ> дозволить підвищити продуктивність захисту, збільшить обсяг оброблюваної інформації на 15%, , скоротити час роботи співробітників з документами, і пошук документів в середньому на 25-30 % за рахунок автоматичного аналізу інформації, наявної в базі даних.

Використання інформаційної системи дозволить більш глибоко і в повному обсязі збирати і аналізувати необхідну інформацію про запити, співробітників.

Відзначено також підвищення ефективності обліку конфіденційної інформації. Одним з найголовніших якісних результатів є те, що у адміністратора безпеки, який несе найбільшу відповідальність за правильність обліку і доступу, є повне уявлення про запити, клієнтів, оскільки він сам оперативно організовує і контролює облік. При цьому в практику роботи персоналу входять нові інформаційні технології, такі як спільний авторизований доступ до довідкової інформації про наявність необхідних даних в БД, автоматизація рутинних операцій, доступ до інформаційно-довідкових ресурсів, стандартизація обліку.

Для швидкої і повної адаптації користувача до системи був розроблений зручний інтерфейс користувача і докладний опис роботи з системою в керівництві користувача.

Вважаю, що створений в дипломному проекті захист персональних даних на підприємстві ТОВ <ЕСКО ><ЕКО-ІДЕЯ> повністю відповідає інформаційним вимогам підприємства і зможе підтримувати це відповідність протягом усього життєвого циклу системи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Базова модель загроз безпеки персональних даних при їх обробці в інформаційних системах персональних даних ‘

2. Виробнича, переддипломна та магістерська практики : метод. вказівки для студ. спеціальності 123 “Комп’ютерна інженерія” / В. М. Джулій, В. О. Бойчук. – Хмельницький : ХНУ, 2010. – 68 с.

3. Домарьов В.В. Безпека інформаційних технологій. Методологія створення систем захисту. - К .: ТОВ ‘ТИД’ ДС ‘, 2010.

4. Директива 95/46 / ЄС Європейського парламенту та Ради Європейського Союзу від 24 жовтня 2003 г. ‘Про захист прав приватних осіб стосовно обробки персональних даних та про вільний рух таких даних. // http: // www.gdf.ru.

5. ДСТУ ГОСТ 7.1:2006. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання. – На заміну ГОСТ 7.1– 84, ГОСТ 7.18–79, ГОСТ 7.34–81, ГОСТ 7.40–82 ; чинний від 2007– 07–01. – Київ : Держспоживстандарт України, 2007. – 47 с.

6. Молдов’ян А.А. Криптографія для захисту комп'ютерної інформації (частина 1) // Інтеграл. 2014. № 4 (18) .

7. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХНУ, 2020. – 196 с.

8. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. – Чинний від 20 грудня 2000 р. – Київ : ДСТСЗІ СБ, 2000. – [8] с.

9. НД ТЗІ 2.7-011-2012. Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. – Чинний від 23 липня 2012 р. – Київ : Адміністрація Держ – спец зв’язку, 2012. – [18] с.

10. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – Чинний від 28 квітня 1999 р. – Київ : ДСТСЗІ СБ, 1999. – [35] с.

11. Романов О.А., Бабин С.А., Жданов С.Г. Організаційне забезпечення інформаційної безпеки. - М .: Академія, 2015

12. Текстові документи. Загальні вимоги. СОУ 207.01:2017 / Ю. Бойко, Г. Красильникова, Л. Першина, Т. Касянчук. – Хмельницький : ХНУ, 2017. – 40 с.

13. Т. Фурашев В.М. Ключові аспекти проекту Закону України “Про безпеку інформації” // “Віче”. – 2012. – № 6/2012(315). – С. 29 – 30.

14. Тимчасове положення про запобігання та виявлення плагіату у Хмельницькому національному університеті від 28.04.2016 р.

15. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ ‘КПІ’, 2016. - 104 с.

16. Савінцева М. Правовий захист персональної інформації громадян. //http://www.medialaw.ru.

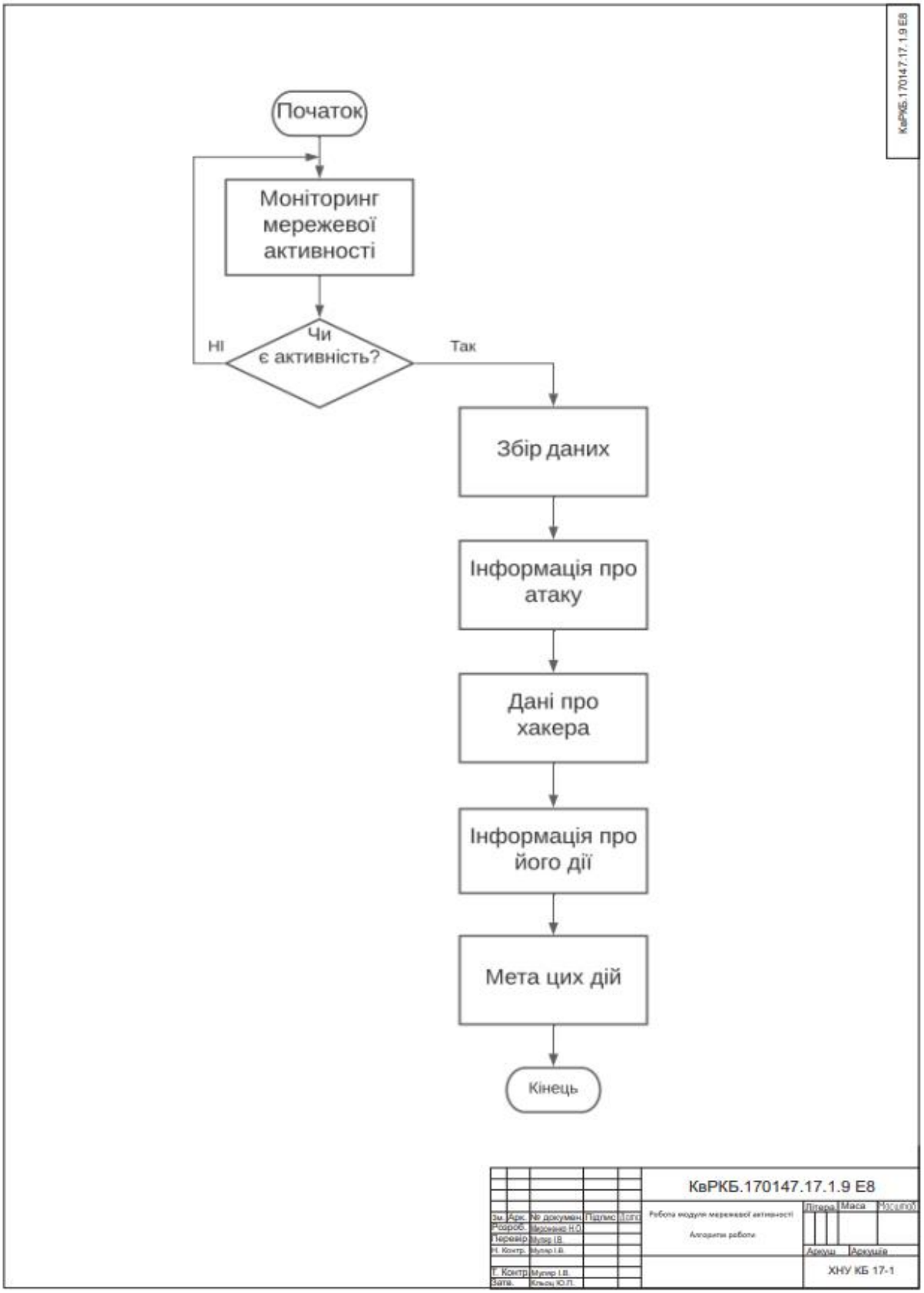
17. Закон України ‘Про електронні документи та електронний документообіг’ // База даних ‘Законодавство України’ / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/851-15

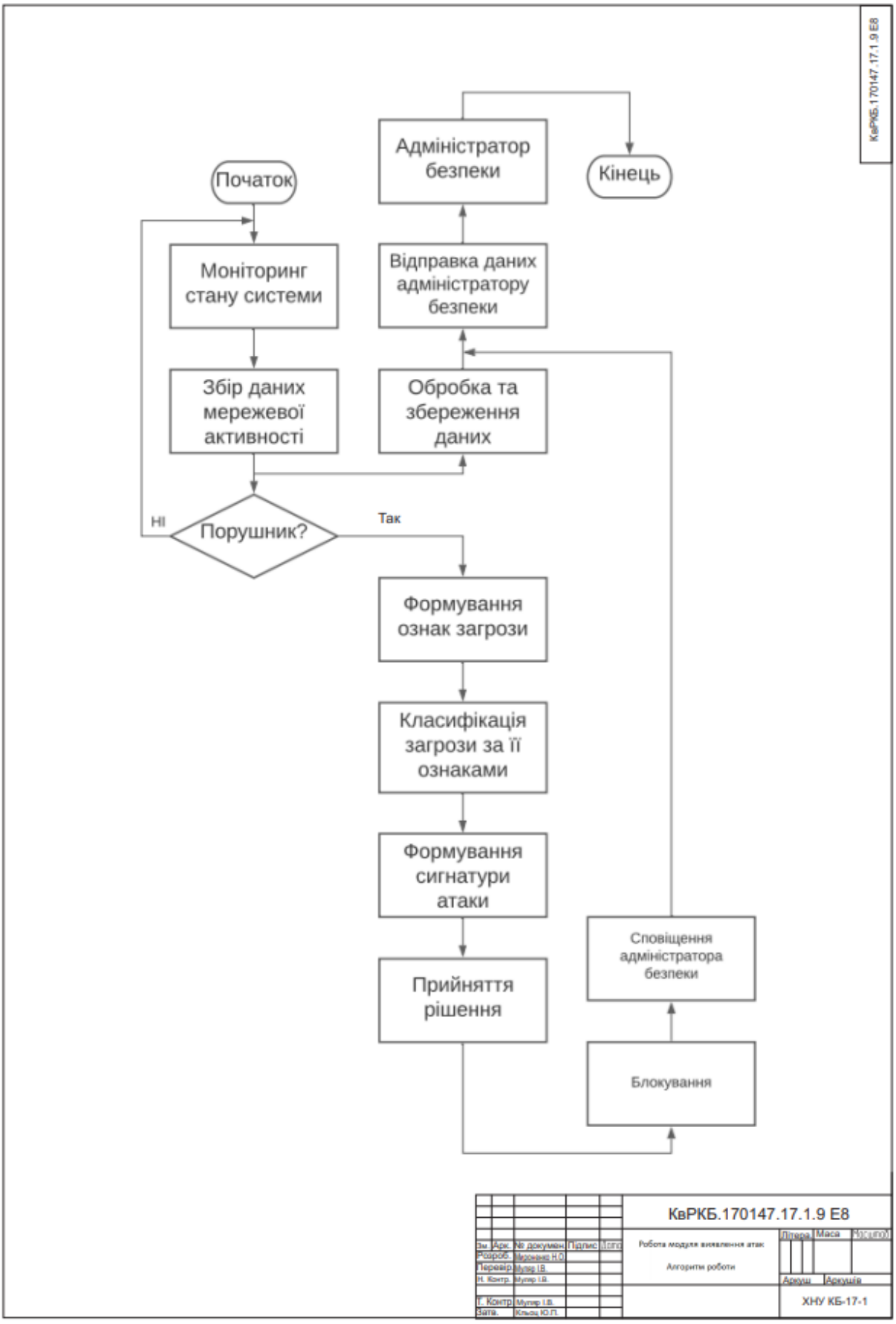
18. Інформаційна безпека Автор:За ред. Ю. Я. Бобала та І. В. Горбатого Видавництво: Львівська політехніка Рік видання: 2019 Сторінок: 580.

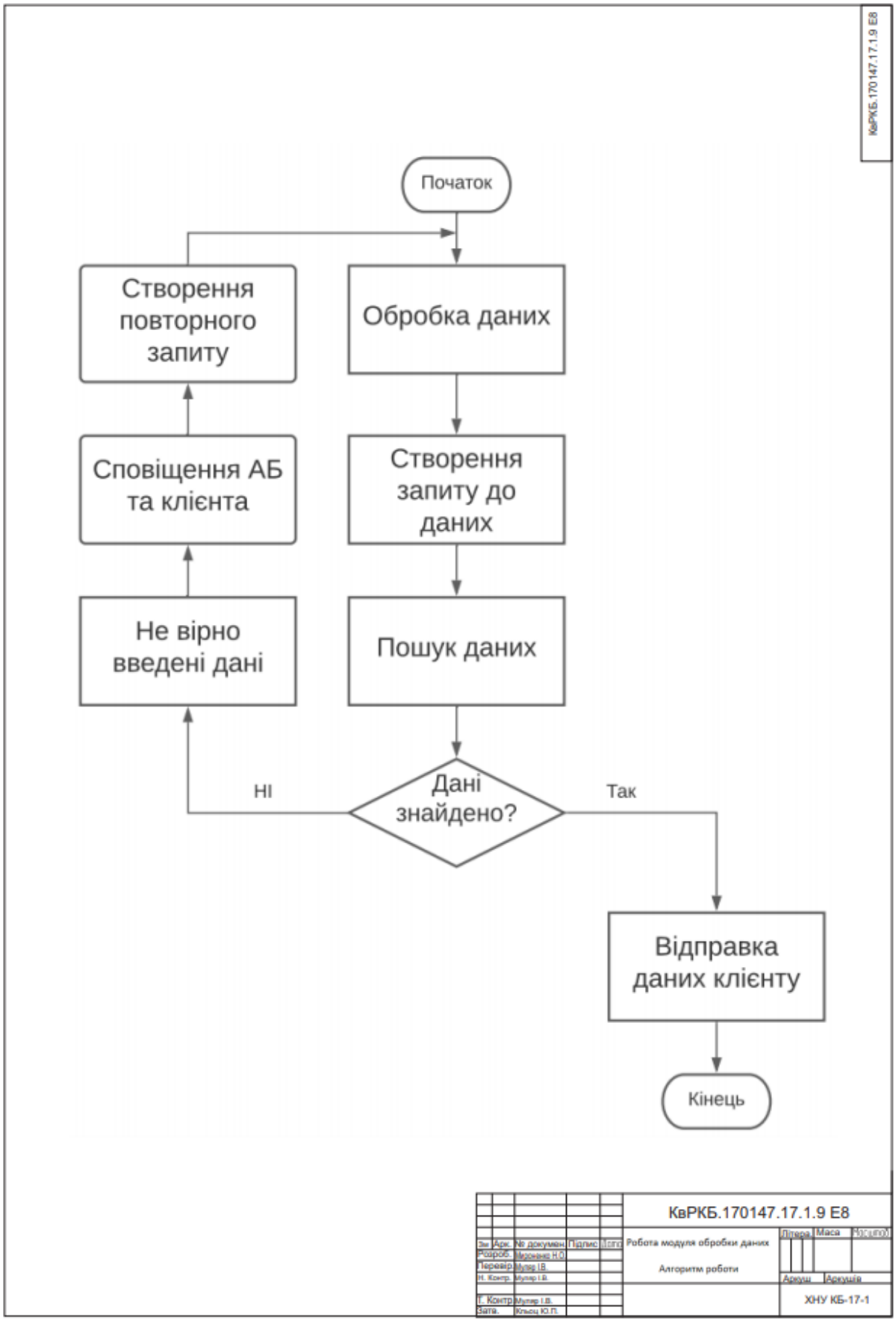
ДОДАТОК А

(Обов’язковий)

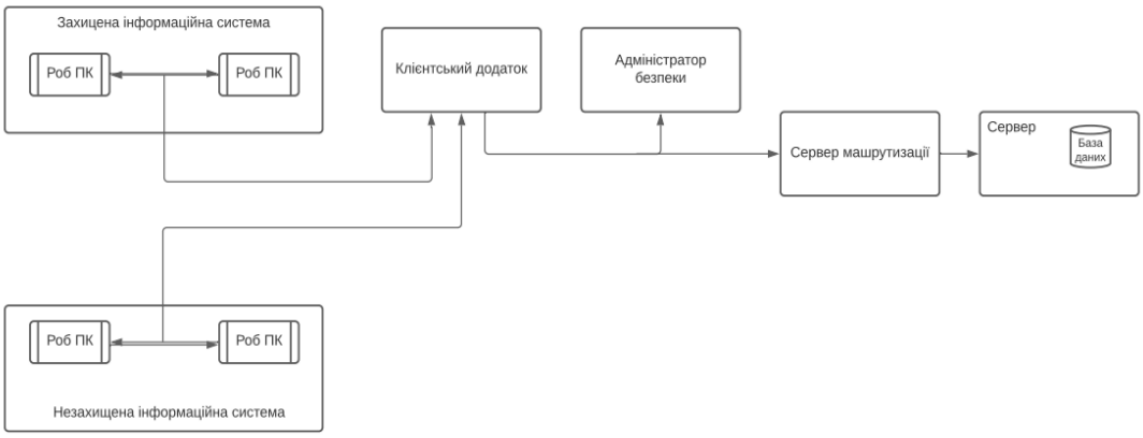
Копія графічної частини




КвРКБ.170147.17.1.9 Е8
Початок
Моніторинг стану системи
Збір даних мережевої активності
Порушник?
НІ
Так
Формування ознак загрози
Класифікація загрози за її ознаками
Формування сигнатури атаки
Прийняття рішення
Блокування
Сповіщення адміністратора безпеки
Обробка та збереження даних
Відправка даних адміністратору безпеки
Адміністратор безпеки
Кінець
КвРКБ.170147.17.1.9 Е8
Робота модуля виявлення атак
Алгоритм роботи
Літера
Маса
Масштаб
Аркуш
Аркушів
ХНУ КБ-17-1
Розроб.
Перевір.
Н. Контр.
Т. Контр.
Затв.

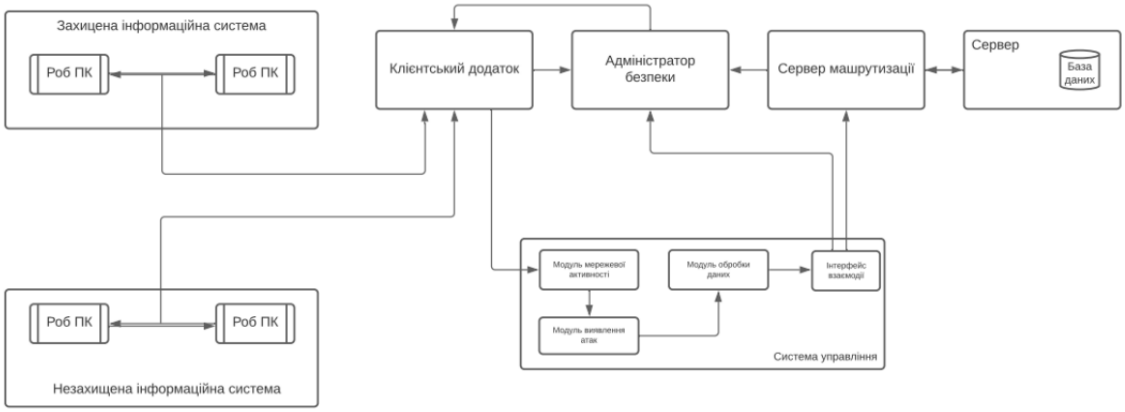

КвРКБ.170147.17.1.9 Е8
Початок
Створення повторного запиту
Обробка даних
Сповіщення АБ та клієнта
Створення запиту до даних
Не вірно введені дані
Пошук даних
НІ
Дані знайдено?
Так
Відправка даних клієнту
Кінець
КвРКБ.170147.17.1.9 Е8
Робота модуля обробки даних
Алгоритм роботи
Літера
Маса
Масштаб
Аркуш
Аркушів
ХНУ КБ-17-1

КвРКБ.170147.17.1.9 Е8



					КвРКБ.170147.17.1.9 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Архітектура системи захисту персональних даних на підприємстві	Літера.	Маса	Масштаб
Розроб.		Мироненко Н.О.						
Перевір.		Мулер І.В.			Схема структурна	Аркуш	Аркушів	
Н. Контр.		Мулер І.В.						
Т. Контр.						ХНУ КБ-17-1		
Затв.		Кільок Ю.П.						

КвРКБ.170147.17.1.9 Е8



					КвРКБ.170147.17.1.9 Е8		
Зм.	Арк.	№ докумен.	Підпис	Дата	Архітектура системи захисту персональних даних на підприємстві модифікована	Літера	Маса	Масштаб
Розроб.		Мироненко Н.О.						
Перевір.		Мулер І.В.			Схема структурна			
Н. Контр.		Мулер І.В.				Аркуш	Аркушів	
Т. Контр.		Мулер І.В.				ХНУ КБ-17-1		
Затв.		Кльов Ю.Л.						

ДОДАТОК Б

(Обов’язковий)

Програмна реалізація

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using FirebirdSql.Data.FirebirdClient;

namespace def1
{
   public partial class Client : Form
   {
      public Client()
      {
         InitializeComponent();

      }

      private void pERSONBindingNavigatorSaveItem_Click(object sender, EventArgs e)
      {
         this.Validate();
         this.pERSONBindingSource.EndEdit();
         this.tableAdapterManager.UpdateAll(this.dataSet1);

      }

      private void Client_Load(object sender, EventArgs e)
      {
         // TODO: This line of code loads data into the 'dataSet1.PERSON' table. You can move, or
remove it, as needed.
         this.pERSONTableAdapter.Fill(this.dataSet1.PERSON);
         // TODO: This line of code loads data into the 'dataSet1.PERSON' table. You can move, or
remove it, as needed.
         this.pERSONTableAdapter.Fill(this.dataSet1.PERSON);
         // TODO: This line of code loads data into the 'dataSet1.PERSON' table. You can move, or
remove it, as needed.
        // this.pERSONTableAdapter.Fill(this.dataSet1.PERSON);


      }

      private void pERSONBindingNavigatorSaveItem_Click_1(object sender, EventArgs e)
      {
         this.Validate();
         this.pERSONBindingSource.EndEdit();
```

```
            this.tableAdapterManager.UpdateAll(this.dataSet1);

        }

        private void button1_Click(object sender, EventArgs e)
        {
            NewClient nc = new NewClient();
            nc.Show();
        }

        private void pERSONBindingNavigatorSaveItem_Click_2(object sender, EventArgs e)
        {
            this.Validate();
            this.pERSONBindingSource.EndEdit();
            this.tableAdapterManager.UpdateAll(this.dataSet1);

        }

        private void pERSONDataGridView_CellContentDoubleClick(object sender,
DataGridViewCellEventArgs e)
        {
            try
            {
                NewReserv nr = (NewReserv)this.Owner;
                if (pERSONDataGridView.CurrentCell != null && pERSONDataGridView.CurrentCell.Value
!= null)
                {
                    nr.textBox1.Text = pERSONDataGridView.Rows[e.RowIndex].Cells[1].Value.ToString();
                    nr.id_client =
Convert.ToInt32(pERSONDataGridView.Rows[e.RowIndex].Cells[0].Value.ToString());
                    Close();
                }
            }
            catch(System.InvalidCastException)
            {
            }
            try
            {
                Occupation nr = (Occupation)this.Owner;
                if (pERSONDataGridView.CurrentCell != null && pERSONDataGridView.CurrentCell.Value
!= null)
                {
                    nr.textBox1.Text = pERSONDataGridView.Rows[e.RowIndex].Cells[1].Value.ToString();
                    nr.id_client =
Convert.ToInt32(pERSONDataGridView.Rows[e.RowIndex].Cells[0].Value.ToString());
                    Close();
                }
            }
            catch (System.InvalidCastException)
            {
            }
            try
            {
                Client_Service cs = (Client_Service)this.Owner;
                if (pERSONDataGridView.CurrentCell != null && pERSONDataGridView.CurrentCell.Value
!= null)
                {
```

```
                cs.textBox1.Text = pERSONDataGridView.Rows[e.RowIndex].Cells[0].Value.ToString();
                Close();
            }
        }
        catch (System.InvalidCastException)
        {
        }
        try
        {
            ReportClient cs = (ReportClient)this.Owner;
            if (pERSONDataGridView.CurrentCell != null && pERSONDataGridView.CurrentCell.Value
!= null)
            {
                cs.textBox1.Text = pERSONDataGridView.Rows[e.RowIndex].Cells[0].Value.ToString();
                Close();
            }
        }
        catch (System.InvalidCastException)
        {
        }
    }

    private void textBox1_TextChanged(object sender, EventArgs e)
    {
        if (pERSONDataGridView.DataSource == pERSONBindingSource)
        {
            pERSONBindingSource.Filter = "[surname]LIKE'" + textBox1.Text + "%'";
        }
    }

    private void удалитьToolStripMenuItem_Click(object sender, EventArgs e)
    {
        if (pERSONDataGridView.RowCount <= 0)
            return;
        DataRow del = ((DataRowView)pERSONBindingSource.Current).Row;
        string message = "Вы действительно хотите удалить клиента?";
        string caption = "Удаление";
        MessageBoxButtons buttons = MessageBoxButtons.OKCancel;

        MessageBoxIcon icon = MessageBoxIcon.Question;
        // Show message box
        DialogResult result = MessageBox.Show(message, caption, buttons, icon);

        if (result == DialogResult.OK)
        {

            FbCommandBuilder fbCommandBuilder = new
FbCommandBuilder(pERSONTableAdapter.Adapter);
            del.Delete();
            pERSONBindingSource.EndEdit();
            pERSONTableAdapter.Adapter.Update(dataSet1, "PERSON");
        }
    }

    private void добавитьИностранцаToolStripMenuItem_Click(object sender, EventArgs e)
    {
        Foreigner f = new Foreigner();
```

```
            f.ShowDialog();
        }

public void AddBtn_Click(object sender, EventArgs e)
        {
            Form1 main = this.Owner as Form1;
            if (main != null)
            {
                DataRow nRow = main.testDataSet.Tables[0].NewRow();
                int rc = main.dataGridView1.RowCount + 1;
                nRow[0] = rc;
                nRow[1] = tbName.Text;
                nRow[2] = tbPhone.Text;
                nRow[3] = tbMail.Text;
                nRow[4] = tbPhoto.Text;
                main.testDataSet.Tables[0].Rows.Add(nRow);
                main.contactsTableAdapter.Update(main.testDataSet.contacts);
                main.testDataSet.Tables[0].AcceptChanges();
                main.dataGridView1.Refresh();
                tbName.Text = "";
                tbPhone.Text = "";
                tbMail.Text = "";
                tbPhoto.Text = "";
            }
        }

        private void добавитьToolStripMenuItem_Click(object sender, EventArgs e)
        {

        }
    }
}
namespace ServerSignalR.Models
{
    public class ApplicationContext : IdentityDbContext<User, Role, Guid>
    {
        public DbSet<Notify> Notifies { get; set; }
        public DbSet<Text> Texts { get; set; }
        public DbSet<Token> Tokens { get; set; }

        public ApplicationContext(DbContextOptions<ApplicationContext> options)
            : base(options)
        {
            Database.EnsureCreated();
        }
        protected override void OnModelCreating(ModelBuilder modelBuilder)
        {
            modelBuilder.Entity<User>().Property(p => p.Id).ValueGeneratedOnAdd();
            base.OnModelCreating(modelBuilder);
        }
    }
}
    public class User:IdentityUser<Guid>
    {

    }
}
```

```
using System;
using System.Collections.Generic;

namespace ServerSignalR.Models
{
   public class Token
   {
      public Guid Id { get; set; }
      public string Value { get; set; }
      public List<Text> Texts { get; set; }
   }
}
using System;
using System.Collections.Generic;

namespace ServerSignalR.Models
{
   public class Text
   {
      public Guid Id { get; set; }
      public string Name { get; set; }
      public LevelConfidence LevelConfidence { get; set; }
      public Guid UserId { get; set; }
      public User User { get; set; }
      public List<Token > Tokens { get; set; }
   }
}
using System;
using System.Collections.Generic;
using System.Linq;
using System.Threading.Tasks;

namespace ServerSignalR.Models
{
   public class Notify
   {
      public Guid Id { get; set; }
      public DateTime DateTime { get; set; }
      public string Message { get; set; }
      public Guid UserId { get; set; }
      public User User { get; set; }
      public NotifyType NotifyType { get; set; }
   }
}
using Microsoft.AspNetCore.Mvc;
using Microsoft.EntityFrameworkCore;
using Microsoft.IdentityModel.Tokens;
using ServerSignalR.JWT;
using ServerSignalR.Models;
using System;
using System.Collections.Generic;
using System.IdentityModel.Tokens.Jwt;
using System.Security.Claims;
using System.Threading.Tasks;

namespace ServerSignalR.Controllers
{
```

```
   public class AccountController : Controller
   {
      private ApplicationContext _context;
      public AccountController(ApplicationContext context)
      {
         _context = context;
      }
      [HttpPost("/token")]
      public async Task<IActionResult> Token(string username, string password)
      {
         var identity = await GetIdentity(username, password);
         if (identity == null)
         {
            return BadRequest("Invalid username or password.");
         }

         var now = DateTime.UtcNow;
         var jwt = new JwtSecurityToken(
               issuer: AuthOptions.ISSUER,
               audience: AuthOptions.AUDIENCE,
               notBefore: now,
               claims: identity.Claims,
               expires: now.Add(TimeSpan.FromMinutes(AuthOptions.LIFETIME)),
               signingCredentials: new SigningCredentials(AuthOptions.GetSymmetricSecurityKey(),
SecurityAlgorithms.HmacSha256));
         var encodedJwt = new JwtSecurityTokenHandler().WriteToken(jwt);

         var response = new
         {
            access_token = encodedJwt,
            username = identity.Name
         };
         return Json(response);
      }

      private async Task<ClaimsIdentity> GetIdentity(string username, string password)
      {
         User person = await _context.Users.Include(r => r.Role).FirstOrDefaultAsync(x => x.Email ==
username && x.Password == password);
         if (person != null)
         {
            var claims = new List<Claim>
            {
               new Claim(ClaimsIdentity.DefaultNameClaimType, person.Email),
               new Claim(ClaimsIdentity.DefaultRoleClaimType, person.Role.Name)
            };
            ClaimsIdentity claimsIdentity =
            new ClaimsIdentity(claims, "Token", ClaimsIdentity.DefaultNameClaimType,
               ClaimsIdentity.DefaultRoleClaimType);
            return claimsIdentity;
         }
         return null;
      }
   }
}
private void button1_Click(object sender, EventArgs e)
    {
```

```
            Form1 main = this.Owner as Form1;
            if (main != null)
            {
               for (int i = 0; i < main.dataGridView1.RowCount; i++)
               {
                  main.dataGridView1.Rows[i].Selected = false;
                  for (int j = 0; j < main.dataGridView1.ColumnCount; j++)
                     if (main.dataGridView1.Rows[i].Cells[j].Value != null)
                     if (main.dataGridView1.Rows[i].Cells[j].Value.ToString().Contains(tbStr.Text))
                        {
                           main.dataGridView1.Rows[i].Selected = true;
                           break;
                        }
               }
            }
      }
private void button3_Click(object sender, EventArgs e)
      {
         Close();
      }
private void button2_Click(object sender, EventArgs e)
      {
         Close();
      }
private void button1_Click(object sender, EventArgs e)
      {
         AddForm af = new AddForm();
         af.Owner = this;
         af.Show();
      }
private void btnGoToAdd_Click (object sender, EventArgs e)
{
   Form frm = new NewCustomer ();
   frm.Show ();
}

/// <summary>
/// Opens the FillorCancel form as a dialog box.
/// </summary>
private void btnGoToFillOrCancel_Click (object sender, EventArgs e)
{
   Form frm = new FillOrCancel ();
   frm.ShowDialog ();
}

/// <summary>
/// Closes the application (not just the Navigation form).
/// </summary>
private void btnExit_Click (object sender, EventArgs e)
{
   this.Close ();
} private int parsedCustomerID;
private int orderID;

/// <summary>
/// Verifies that the customer name text box is not empty.
/// </summary>
```

```
private bool IsCustomerNameValid ()
{
   if (txtCustomerName.Text == "")
   {
      MessageBox.Show ("Please enter a name.");
      return false;
   }
   else
   {
      return true;
   }
}

/// <summary>
/// Verifies that a customer ID and order amount have been provided.
/// </summary>
private bool IsOrderDataValid ()
{
   // Verify that CustomerID is present.
   if (txtCustomerID.Text == "")
   {
      MessageBox.Show ("Please create customer account before placing order.");
      return false;
   }
   // Verify that Amount isn't 0.
   else if ((numOrderAmount.Value <1))
   {
      MessageBox.Show ("Please specify an order amount.");
      return false;
   }
   else
   {
      // Order can be submitted.
      return true;
   }
}

/// <summary>
/// Clears the form data.
/// </summary>
private void ClearForm ()
{
   txtCustomerName.Clear ();
   txtCustomerID.Clear ();
   dtpOrderDate.Value = DateTime.Now;
   numOrderAmount.Value = 0;
   this.parsedCustomerID = 0;
} private void btnCreateAccount_Click (object sender, EventArgs e)
{
   if (IsCustomerNameValid ())
   {
      // Create the connection.
      using (SqlConnection connection = new SqlConnection (Properties.Settings.Default.connString))
      {
         // Create a SqlCommand, and identify it as a stored procedure.
         using (SqlCommand sqlCommand = new SqlCommand ("Sales.uspNewCustomer", connection))
{
```

```
            sqlCommand.CommandType = CommandType.StoredProcedure;

            // Add input parameter for the stored procedure and specify what to use as its value.
            sqlCommand.Parameters.Add(new SqlParameter("@CustomerName", SqlDbType.NVarChar, 40));
            sqlCommand.Parameters["@CustomerName"].Value = txtCustomerName.Text;

            // Add the output parameter.
            sqlCommand.Parameters.Add(new SqlParameter("@CustomerID", SqlDbType.Int));
            sqlCommand.Parameters["@CustomerID"].Direction = ParameterDirection.Output;

            try
            {
               connection.Open();

               // Run the stored procedure.
               sqlCommand.ExecuteNonQuery();

               // Customer ID is an IDENTITY value from the database.
               this.parsedCustomerID = (int)sqlCommand.Parameters["@CustomerID"].Value;

               // Put the Customer ID value into the read-only text box.
               this.txtCustomerID.Text = Convert.ToString(parsedCustomerID);
            }
            catch
            {
               MessageBox.Show("Customer ID was not returned. Account could not be created.");
            }
            finally
            {
               connection.Close();
            }
         }
      }
   }
}

/// <summary>
/// Calls the Sales.uspPlaceNewOrder stored procedure to place an order.
/// </summary>
private void btnPlaceOrder_Click(object sender, EventArgs e)
{
   // Ensure the required input is present.
   if (IsOrderDataValid())
   {
      // Create the connection.
      using (SqlConnection connection = new SqlConnection(Properties.Settings.Default.connString))
      {
         // Create SqlCommand and identify it as a stored procedure.
         using (SqlCommand sqlCommand = new SqlCommand("Sales.uspPlaceNewOrder", connection))
         {
            sqlCommand.CommandType = CommandType.StoredProcedure;

            // Add the @CustomerID input parameter, which was obtained from uspNewCustomer.
            sqlCommand.Parameters.Add(new SqlParameter("@CustomerID", SqlDbType.Int));
            sqlCommand.Parameters["@CustomerID"].Value = this.parsedCustomerID;
sqlCommand.Parameters.Add(new SqlParameter("@OrderDate", SqlDbType.DateTime, 8));
            sqlCommand.Parameters["@OrderDate"].Value = dtpOrderDate.Value;
```

```
            // Add the @Amount order amount input parameter.
            sqlCommand.Parameters.Add(new SqlParameter("@Amount", SqlDbType.Int));
            sqlCommand.Parameters["@Amount"].Value = numOrderAmount.Value;

            // Add the @Status order status input parameter.
            // For a new order, the status is always O (open).
            sqlCommand.Parameters.Add(new SqlParameter("@Status", SqlDbType.Char, 1));
            sqlCommand.Parameters["@Status"].Value = "O";

            // Add the return value for the stored procedure, which is  the order ID.
            sqlCommand.Parameters.Add(new SqlParameter("@RC", SqlDbType.Int));
            sqlCommand.Parameters["@RC"].Direction = ParameterDirection.ReturnValue;

            try
            {
               //Open connection.
               connection.Open();

               // Run the stored procedure.
               sqlCommand.ExecuteNonQuery();

               // Display the order number.
               this.orderID = (int)sqlCommand.Parameters["@RC"].Value;
               MessageBox.Show("Order number " + this.orderID + " has been submitted.");
            }
            catch
            {
               MessageBox.Show("Order could not be placed.");
            }
            finally
            {
               connection.Close();
            }
         }
      }
   }
}

/// <summary>
/// Clears the form data so another new account can be created.
/// </summary>
private void btnAddAnotherAccount_Click(object sender, EventArgs e)
{
   this.ClearForm();
}

/// <summary>
/// Closes the form/dialog box.
/// </summary>
private void btnAddFinish_Click(object sender, EventArgs e)
{
   this.Close();
}
private int parsedOrderID;

/// <summary>
```

```
/// Verifies that an order ID is present and contains valid characters.
/// </summary>
private bool IsOrderIDValid()
{
   // Check for input in the Order ID text box.
   if (txtOrderID.Text == "")
   {
      MessageBox.Show("Please specify the Order ID.");
      return false;
   }

   // Check for characters other than integers.
   else if (Regex.IsMatch(txtOrderID.Text, @"^\D*$"))
   {
      // Show message and clear input.
      MessageBox.Show("Customer ID must contain only numbers.");
      txtOrderID.Clear();
      return false;
   }
   else
   {
      // Convert the text in the text box to an integer to send to the database.
      parsedOrderID = Int32.Parse(txtOrderID.Text);
      return true;
   }
}
```

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Організаціязахиступерсональнихданих в підприємстві ТОВ <ЕСКО><ЕКО-ІДЕЯ>

Автор: Мироненко Назар Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Керівник:Муляр Ігор Володимирович, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та опрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформлені посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає15.4% що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи І.В. Муляр

Завідувач кафедри КбКСМ, гарантОП Ю.П. Кльоц

Дата: 07.06.2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Мироненко Назар Олександрович

Тема Організація захисту персональних даних в підприємстві ТОВ <ЕСКО ЕКО-ІДЕЯ>

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 5; кількість сторінок записки 49

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено систему для захисту персональних даних на підприємстві.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, визначено об'єкт, предмет та методи дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено огляд використовуваних в комп'ютерних системах методів захисту конфіденційної інформації, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі наведені засоби використані для побудови системи захисту. В третьому розділі визначено основні положення системи та розроблено алгоритми її роботи. Четвертий розділ було присвячено апробації системи захисту та алгоритмів її реалізації.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність полягає у розробці модулів мережевої активності, виявлення атак та обробки даних. На основі даного аналізу в подальшому здійснюється керуючий вплив на витік конфіденційних даних. Практична цінність результатів кваліфікаційної роботи полягає у створені системи захисту персональних даних, що може бути підлаштована для будь якої категорії даних, і у описі оптимальних моделей функціонування систем захисту подібного характеру.

5. Негативні сторони роботи Розроблена система захисту персональних даних досить чутлива до навантаження. В роботі мало уваги надається технічній реалізації системи (програмній, програмно-апаратній).

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Лисенко Сергій Миколайович доктор технічних наук інженер та доцент за кафедрою системного програмування.

«20» червня 2021. (підпис)

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008317179

Check date:
17.06.2021 09:56:52 EEST

Check type:
Doc vs Internet

Report date:
17.06.2021 09:57:26 EEST

User ID:
100005590

File name: **Кваліфікайійна робота Мироненко пл**

Page count: **49** Word count: **7921** Character count: **60008** File size: **585.50 KB** File ID: **1008384296**

15.4% Matches

Highest match: **12.3%** with Internet source (https://ela.kpi.ua/bitstream/123456789/34622/1/Litvin_bakalavr.pdf)

15.4% Internet sources | 243 ..... Page 51

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 2.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 6%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 94423 Название: Організація захисту персональних даних в підприємстві ТОВ <ЕСКО><ЕКО-ІДЕЯ> Добавлено в БД: 2021-06-17 Авторы: Мироненко Н О Руководители: Муляр І.В. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	52283	428	2324 (4%)	29 (7%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы