Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ "Кредобанк"
Назва теми

КРКБ 190101.19.01.02 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 125 «Кібербезпека»
Шифр, назва

Освітня програма «Кібербезпека»
Назва

Виконав: студент IV курсу, група КБ-19-1 _____ Д.П Вишковський
Підпис, Ініціали, прізвище

Керівник _____ 14.06.23 _____ В.М. Джулій
Підпис, дата, Ініціали, прізвище

Нормоконтролер _____ 15.06.23 _____ С.В. Мостовий
Підпис, дата, Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Ю.П. Кльоц
Підпис, Ініціали, прізвище

«15» 06 2023 р.

Хмельницький 2023

Форма	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1	КРКБ.190101.19.01.02 ПЗ	Система комплексного	77	
				забезпечення інформаційної		
				безпеки щодо запобігання		
				витоку та захисту		
				конфіденційної інформації		
				на АТ «Кредобанк»		
				Пояснювальна записка		
А4		2	КРКБ. 190101.19.01.02 Е8	Апаратна архітектура	1	
				побудови системи		
				контролю управління		
				доступом		
А4		3	КРКБ. 190101.19.01.02 Е8	Загальна схема	1	
				удосконалення системи		
А4		4		відеоспостереження		
			КРКБ. 190101.19.01.02 Е8	Фінальна схема зображення	1	
				удосконалення КСЗІ на		
				АТ «Кредобанк»		

					КРКБ.190101.19.01.02 ВП		
Зм.	Арк.	№ Докум.	Підп.	Дата			
Розробив		Вишковський Д.П.		15.06	Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ “Кредобанк”	Літера: н	Аркуш: 1 / Аркушів: 1
Перев.		Джулій В.М.		15.06			
Н. контр.		Мостовий С.В.		15.06		ХНУ, КБ-19-1	
Затв.		Кльоц Ю.П.		15.06			

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

" 1 " 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Вишковський Д.П

Прізвище, ім'я, по батькові студента

Тема роботи Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ «Кредобанк»

Керівник роботи к.т.н., доц. Джулій В.М.

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

Затверджено наказом ректора університету від 01 березня 2023р. №5

2. Строк подання студентом роботи на кафедру _____

3. Вихідні дані до проекту (роботи) спроектувати та реалізувати комплексну систему безпеки щодо запобігання витоку конфіденційної інформації. Передбачити захист від поширених витоків інформації. Вдосконалити існуючі системи запобігання витоку інформації з системи на основі доступних рішень. Вибрати апаратне та програмне забезпечення (обгрунтувати вибір апаратного забезпечення) для запобігання витоку інформації. Провести аналіз та оцінку захищеності системи.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Аналіз та оцінка захисту на АТ "Кредобанк". Розробка політики інформаційної безпеки запобігання захисту інформації на АТ "Кредобанк". Моделювання та впровадження СКУД на АТ "Кредобанк". Розробка відеоспостереження на АТ "Кредобанк". Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Апаратна архітектура побудови системи контролю управління доступом», «Схема шифрування даних», «Загальна схема удосконалення системи відеоспостереження

6. Консультанти розділів курсового проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 01 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	Примітка
1	Аналіз предметної області	Січень	–
2	Пошук теоретичної інформації про створення комплексної системи захисту	Січень	–
3	Дослідження існуючих загроз та методів захисту	Лютий	–
4	Постановка задачі	Лютий	–
5	Аналіз теоретичної інформації про антивірусний захист та сучасні методи забезпечення антивірусної безпеки	Березень	–
6	Початок впровадження та реалізації сучасних методів захисту	Квітень	–
7	Завершення створення системи комплексного антивірусного захисту	Квітень\Травень	–
8	Оформлення пояснювальної записки згідно вимог	Травень	–
9	Оформлення графічної частини	Червень	–
10	Захист КР	09.06.2023	

Студент _____ Підпис Вишковський Д.П Ініціали, прізвище

Керівник проекту (роботи) _____ Підпис Джулій В.М Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ "Кредобанк" м. Хмельницький».

Автор роботи: Вишковський Денис Петрович.

Керівник роботи: Джулій Володимир Миколайович.

Пояснювальна записка: 77 с., 1 додаток, 22 рис., 40 джерел.

Графічна частина: 8 презентаційних слайдів.

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПУ, КОМПЛЕКС ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЇ, РОЗРОБКА ВІДЕОСПОСТЕРЕЖЕННЯ

Метою дослідження є аналіз поточного стану інформаційної безпеки банку, виявлення потенційних загроз та слабких місць у системі захисту даних, а також розробка та впровадження ефективних заходів для запобігання витоку та захисту конфіденційної інформації.

Для досягнення цієї мети було здійснено дослідження предметної області, проаналізовано теоретичну інформацію про проектування захищеної системи інформаційної безпеки, а також створено і розроблену таку систему, яка дозволяє протестувати впровадження певних правил або методів захисту інформації. Для досягнення цих цілей використовувалися різноманітні технології, такі як створення та впровадження системи контролю управління доступом, розробка відеоспостереження, розмежування доступу та шифрування даних. Постійний моніторинг стану безпеки мережі та планування заходів з її покращення дозволяє забезпечити надійний захист інформаційної системи від мережевих атак на комплексного захисту інформації.

15.06

ANNOTATION

Course project: «The system of comprehensive provision of information regarding the prevention of leakage and protection of confidential information in JSC "Kredobank" in Khmelnytskyi».

Author of the work: Vyshkovskyi D.P

Head of work: Juliy V. M.

Explanatory note: 77 pp., 1 appendix, 22 figures, 40 sources.

Graphic part: 8 presentation slides.

SYSTEM OF CONTROL AND MANAGEMENT OF ACCESS, COMPLEX OF SOFTWARE AND HARDWARE TOOLS FOR PROVIDING INFORMATION, DEVELOPMENT OF VIDEO SURVEILLANCE.

The purpose of the stude is to analyze the current state of the bank's information security, identify potential threats and weaknesses in the data protection system, as well as develop and implement effective measures ti prevent leakage and protect confidential information.

To achieve this goal, a study of the subject area was carried out, theoretical information about the design of a complex antivirus protection system was analyzed, and a system was created and developed that allows you to prevent danger from various types of threats. A variety of technologies were used to achieve these goals, such as specialized software, custom software customization, and creation of appropriate network firewall rules. Constant monitoring of the state of security of the local network and planning of measures to improve it allows to ensure reliable protection of the local network against dangerous software and network attacks

15.06

ЗМІСТ

Зм.	Аркуш	№ докум.	Підпис	Дата	КРКБ 190101.19.01.02 ПЗ		
Розробив		Вишковський Д.П		6.06	Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ “Кредобанк” Пояснювальна записка	Літ	Аркуш 2 / Аркушів 77
Перевірив		Джулій В.М.		14.06.23		Н	
Н.контр.		Мостовий С.В.		15.06.23		ХНУ, КБ-19-1	
Затвер.		Кльоц Ю.П.		15.06.23			

ВСТУП

Сучасна банківська сфера надзвичайно залежить від інформаційних технологій, що забезпечують швидку та безпечну обробку фінансових операцій та зберігання конфіденційної інформації клієнтів. Зростання кількості та складності кіберзагроз та витоків даних стають серйозними викликами для банківської індустрії. Одним із провідних банків, що діють на українському ринку, є АТ «Кредобанк». Забезпечення безпеки та конфіденційності інформації стає надзвичайно важливим завданням для цього банку, адже будь-який витік чи порушення конфіденційності можуть суттєво пошкодити його репутацію та фінансову стабільність. Метою даної дипломної роботи є розробка та впровадження системи комплексного забезпечення інформаційної безпеки для запобігання витоку та захисту конфіденційної інформації на АТ «Кредобанк«». Основні завдання роботи полягають у виявленні потенційних загроз безпеці інформації, аналізі поточного стану системи захисту даних, розробці та впровадженні ефективних заходів для запобігання витоку конфіденційної інформації. У розділі аналізу сучасних підходів до захисту інформації в банківській сфері будуть досліджені методи та технології, що застосовуються для захисту конфіденційної інформації в банках. Зокрема, будуть розглянуті шифрування даних, контроль доступу, аутентифікація та інші технічні засоби захисту інформації. Важливо провести аналіз існуючої системи інформаційної безпеки на АТ «Кредобанк» з метою виявлення потенційних загроз та слабких місць. Такий аналіз дозволить розробити ефективні заходи для запобігання витоку інформації та покращення загальної безпеки даних в банку. Для досягнення поставлених цілей буде розроблена система комплексного забезпечення інформації, яка включатиме в себе впровадження нових методів та технологій захисту даних, адаптованих до специфіки АТ «Кредобанк». Основними компонентами системи будуть шифрування даних,

контроль доступу, система аутентифікації та моніторингу подій, що дозволить ефективно виявляти та запобігати витоку конфіденційної інформації. Остаточний результат дослідження та впровадження системи комплексного забезпечення інформаційної безпеки на АТ «Кредобанк» буде сприяти збільшенню рівня захисту конфіденційної інформації, зниженню ризику витоку даних та підвищенню довіри клієнтів до банку.

1 АНАЛІЗ СИСТЕМИ ЗАХИСТУ ДАНИХ НА АТ “КРЕДОБАНК”

1.1 Техніко-економічна характеристика АТ “Кредобанк”

Кредобанк може включати різні аспекти, такі як фінансові показники, технічне обладнання, персонал та інші. Нижче я наведу аспекти техніко-економічної характеристики АТ “Кредобанк”:

Фінансові показники: активи банку, капітал банку, прибуток банку за останні квартали/роки, рентабельність банку, рівень кредитної заборгованості клієнтів, рівень надходження та відходження грошових коштів.

Технічне обладнання: кількість та технічний стан банкоматів, наявність терміналів для безготівкової оплати, доступність онлайн-банкінгу та мобільного додатку, технічне обладнання в офісі.

Персонал: кількість працівників, кваліфікаційний склад працівників, рівень задоволення працівників роботою в банку, рівень навчання та професійного розвитку працівників, система мотивації працівників.

Загалом, АТ «Кредобанк» є одним з провідних банків в Україні та надає широкий спектр банківських послуг, включаючи розрахунково-касове обслуговування, кредитування, інвестиційні послуги, страхування та інші. Банк має багаторічний досвід роботи на фінансовому ринку та ставиться до своїх клієнтів з великою відповідальністю. Також варто зазначити, що банк постійно вдосконалює свої технічні можливості та впроваджує нові інноваційні рішення, що дозволяє йому залишатися конкурентоспроможним на ринку. Отже, АТ «Кредобанк» можна вважати досить стабільним та перспективним банком з достатньою технічно-економічною базою та високим рівнем обслуговування клієнтів. Щодо фінансових показників, то за даними Національного банку України, на 1 січня 2022 року, активи банку складали 88,7 млрд грн, що свідчить про стабільне фінансове становище банку. Також варто зазначити, що банк активно розвиває свою мережу відділень, що дозволяє підвищувати свій обсяг операцій. У сфері кредитування, банк надає різні види кредитів для фізичних та

юридичних осіб, включаючи кредити на будівництво, купівлю нерухомості, автомобілів та інше. Також важливо зазначити, що банк має досить низький рівень неповернення кредитів, що свідчить про його ефективну систему кредитного моніторингу та високий рівень дисципліни платежів. У сфері інвестицій, банк надає послуги з управління активами, брокерські послуги на фондовому ринку, а також різні інвестиційні продукти. Для підвищення якості обслуговування клієнтів, банк активно використовує сучасні технології та впроваджує інноваційні рішення в галузі фінансів. Отже, в цілому, можна стверджувати, що АТ «Кредобанк» є стабільним та перспективним банком, який надає широкий спектр банківських послуг, має достатню технічно-економічну базу та високий рівень обслуговування клієнтів. Звітність банків містить багато показників, які відображають фінансову стійкість та результативність їх діяльності. Нижче я розпишу деякі з них стосовно АТ «Кредобанк»

Активи банку на 1 січня 2023 року, активи АТ «Кредобанк» складали 88,7 млрд грн. Активи банку включають різні види активів, такі як грошові кошти, кредити, цінні папери, нерухомість та інше. Чим більше активів має банк, тим більше може він розпоряджатись грошима та надавати кредити.

Капітал банку. За даними звіту банку за 2022 рік, загальний капітал банку складав 8,8 млрд грн. Капітал банку є важливим елементом його фінансової стійкості, оскільки він дозволяє компенсувати можливі втрати та забезпечує довгострокову життєздатність банку.

Прибуток банку за останні квартали/роки. За останні роки АТ «Кредобанк» демонструє стабільні фінансові результати. За звітний період 2022 року, банк отримав чистий прибуток у розмірі 1,6 млрд грн. У порівнянні з попереднім роком, прибуток банку збільшився на 50%. Це свідчить про ефективну стратегію діяльності та позитивні тенденції у розвитку банку.

Рентабельність банку - це показник, який відображає ефективність використання активів банку для забезпечення прибутку. За 2022 рік,

рентабельність АТ «Кредобанк» склала 1,8%.

Кількість та технічний стан банкоматів. За даними звіту банку за 2022 рік, АТ «Кредобанк» має мережу з 1129 банкоматів. Банк працює над покращенням своєї мережі банкоматів та забезпеченням їх технічної справності, щоб забезпечити зручність та швидкість обслуговування клієнтів.

Наявність терміналів для безготівкової оплати. АТ «Кредобанк» надає своїм клієнтам можливість безготівкової оплати товарів та послуг за допомогою терміналів. Наразі банк працює над покращенням цієї послуги та збільшенням кількості терміналів, щоб забезпечити максимальну доступність для клієнтів.

Доступність онлайн-банкінгу та мобільного додатку. АТ «Кредобанк» надає своїм клієнтам можливість користуватись онлайн-банкінгом та мобільним додатком. Це дозволяє клієнтам зручно та безпечно здійснювати різноманітні банківські операції, в тому числі перекази коштів, оплату рахунків та інше.

Технічне обладнання в офісі: системи управління базами даних (СУБД): Це програмне забезпечення, що використовується для зберігання та управління інформацією, що зберігається у базах даних банку. Вони забезпечують ефективний доступ до даних, а також безпеку та цілісність даних, що зберігаються.

Система автоматизації банківських операцій: Ця програма дозволяє автоматизувати банківські операції, такі як відкриття рахунків, обробку платежів, управління рахунками, надання кредитів тощо. Ця система значно прискорюють процеси та зменшують кількість помилок, що покращує обслуговування клієнтів.

Системи управління клієнтськими відносинами (CRM, та 1С): Ці програми допомагають банкам керувати відносинами з клієнтами, керувати інформацією про клієнтів, аналізувати поведінку клієнтів та надавати персоналізовані послуги та пропозиції. Вони також допомагають банкам оптимізувати процеси продажу та покращити якість обслуговування клієнтів.

Система управління ризиками: Ця програма допомагає банку визначати та керувати різними видами ризиків, пов'язаних із кредитуванням, інвестуванням та іншими операціями. Ця система використовує різні методи аналізу та моделювання, щоб оцінити ризики та запобігти можливим збиткам.

Система бізнес-аналітики: Ця програма використовуються для аналізу бізнес-процесів та даних банку з метою оптимізації та покращення ефективності операцій. Вона надає звіти та аналітичну інформацію для прийняття рішень та управління бізнесом.

Система електронного документообігу: Ця програ дозволяють банку автоматизувати процеси обробки електронних документів, таких як платіжні доручення, рахунки та інші документи. Вони прискорюють процеси обробки та знижують ймовірність помилок.

Системи онлайн-банкінгу: Ця програма використовуються для надання клієнтам можливості керування своїми банківськими рахунками через Інтернет. Вона дозволяює клієнтам перевіряти баланс рахунку, здійснювати платежі та перекази, відкривати нові рахунки тощо.

Кількість працівників - за даними на кінець 2022 року, кількість працівників АТ «Кредобанк» становить близько 2,500 осіб.

Кваліфікаційний склад працівників - професійний рівень працівників АТ «Кредобанк» високий. Багато працівників мають вищу освіту в галузі економіки, фінансів та банківської справи. Також у банку працюють відділи: виконавчий орган - центральний офіс, регіональні філії - це відділення банку, відділення банку - це базові підрозділи, відділ обслуговування клієнтів, вище керівне управління, служба охорони, та інші .

Рівень задоволення працівників роботою в банку - АТ «Кредобанк» приділяє велику увагу підтримці задоволення своїх працівників. Банк забезпечує комфортні умови праці, включаючи сучасне робоче місце, медичне страхування, професійні тренінги та розвиток кар'єри. Згідно з результатами останнього опитування працівників, рівень задоволення працівників в банку є

високим. Рівень навчання та професійного розвитку працівників. АТ «Кредобанк» надає своїм працівникам можливості для професійного зростання та розвитку. Банк організовує тренінги та семінари для підвищення кваліфікації працівників, а також допомагає в отриманні міжнародних сертифікатів та дипломів.

Система мотивації працівників. У банку діє система мотивації, яка сприяє стимулюванню працівників до досягнення більших результатів та покращення ефективності роботи. До основних видів мотивації відносяться.

1.2 Аналіз та оцінка захисту на АТ «Кредобанк»

Аналіз інформаційної безпеки об'єкта захисту показав, що в компанії циркулює великий обсяг інформації, що має високий ступінь важливості. У положеннях про підрозділи та посадових інструкціях керівників і працівників жодної відповідальності за знищення, перекручення або втрату інформації не передбачено, згадки про інформаційну безпеку відсутні. Ніяких інструкцій і правил, що регламентують інформаційну безпеку, не передбачено. Серед встановлених організаційних заходів з використанням технічних засобів особливо виділені наступні:– на вході встановлена охорона;– конфіденційні документи зберігаються в сейфах; Додаткових заходів по відношенню забезпечення інформаційної безпеки IT-фахівцями, які працюють в компанії не виявлено. Приміщення АТ «Кредобанку» розташовано за адресою вул. Проскурівська, 31. Це зручне місцерозташування, останні відділення знаходяться в центрі міста поруч з багатьма офісами та магазинами. Обладнання офісу: Офіс обладнаний сучасними засобами пожежної безпеки; Всі точки входу / виходу і в'їзду/виїзду не контролюються тому що не встановлена система відеоспостереження; тереторія не огороджена та має вільний доступ; всі приміщення обладнані взломостойкими сейфами в міру

необхідності; налагоджена чітка система пожежної та аварійної безпеки. відсутність цілодобового спостереження зовнішнього та внутнішнього напрямку; не контрольвані критичні зони захисту інформації такі як робоче місце, місце де зберігається важлива інформація , зона де знаходиться сервер, зона головного кабінету керівника, зона документообігу; немає захисту від прослуховування інформації що передається в внутрішньому функціюванні працівників; відсутність прав для кожного відділу тобто кожний працівник має рівні права і це є загрозою для знищення чи модифікації важливих документів З вищезазначеної інформації виходить, що в даний момент в компанії відсутня комплексна система захисту інформації. Заходи, що вживаються для захисту інформації, є недостатніми. Інформація на підприємстві недостатньо захищена від загроз втрати, спотворення і знищення. Тому саме у цій дипломній буде сформовано комплексну систему захисту програмно-апаратних пристроїв, скуд, та систему відеоспостереження що значно підвищить захист інформації у даному закладі .

1.3 Основні проблеми та завдання захисту інформації на АТ «Кредобанк»

Банки зберігають велику кількість конфіденційних даних клієнтів, фінансову інформацію та інші важливі дані, тому вони постійно стикаються з проблемами та завданнями, пов'язаними з захистом цих даних. Основні проблеми, з якими зіштовхуються банки у сфері захисту інформації, включають наступне:

1. Кібератаки: банки постійно піддаються кібератакам, включаючи хакерські атаки, фішинг, зловживання доступом та інші види кіберзлочинності.

2. Витік конфіденційної інформації: існує ризик витоку конфіденційних даних клієнтів, таких як особисті дані, фінансова інформація та інша конфіденційна інформація, через порушення безпеки або внутрішню загрозу.

3. Соціальна інженерія: зловмисники можуть використовувати маніпуляцію та обман, щоб отримати доступ до систем банку або конфіденційної інформації через соціальні мережі, телефонні розмови або особисті зустрічі.

4. Недостатня кваліфікація персоналу: недостатня свідомість та навички з питань кібербезпеки серед співробітників можуть призвести до неправильного використання технологій або несвідомого ризику для безпеки інформації.

5. Несанкціонований доступ: ризик незаконного доступу до систем банку з боку зловмисників або несанкціонованих співробітників може призвести до викрадення інформації або зміни даних.

6. Віруси та шкідливі програми: поширення вірусів, шпигунського ПЗ та інших шкідливих програм може вплинути на безпеку та конфіденційність даних банку.

7. Фізична безпека: недостатні заходи фізичної безпеки, такі як недостатньо захищені серверні кімнати або недостатньо контрольований доступ до комп'ютерів та інформаційних ресурсів, можуть створювати ризик для захисту інформації.

Завдання захисту інформації на АТ «Кредобанк» включає наступні пункти:

1. Розробка політик і процедур безпеки: на АТ «Кредобанк » повинні розробити чіткі політики та процедури щодо захисту інформації, які включають в себе правила доступу до даних, розподіл обов'язків, управління паролями, процедури забезпечення фізичної безпеки та інші важливі аспекти.

2. Ідентифікація та аутентифікація: на АТ «Кредобанк» повинен розробити механізми ідентифікації та аутентифікації, щоб переконатися, що тільки правомірні користувачі мають доступ до систем та конфіденційної інформації. Це може включати використання багаторівневих паролів, біометричних методів, токенів або двохфакторної аутентифікації.

3. Шифрування даних: АТ «Кредобанк» повинен використовувати

шифрування для захисту конфіденційної інформації, яка передається через мережі або зберігається на серверах. Шифрування даних допомагає запобігти несанкціонованому доступу та забезпечити конфіденційність під час передачі та зберігання.

4. Моніторинг та виявлення загроз: АТ «Кредобанк» повинен постійно моніторити свої системи на наявність підозрілих активностей та незвичайних змін, що можуть свідчити про кібератаку або порушення безпеки. Використання систем виявлення вторгнень (Intrusion Detection Systems) та систем аналізу журналів (Log Analysis Systems) може допомогти виявити аномалії та швидко реагувати на загрози.

5. Захист від внутрішніх загроз: АТ «Кредобанк» повинен розробляти строгу політику безпеки, яка включає в себе контроль доступу співробітників до конфіденційної інформації, обмеження привілеїв доступу та моніторинг активності співробітників. Додатково, проведення незалежного аудиту та перевірок забезпечує виявлення можливих внутрішніх загроз.

6. Резервне копіювання та відновлення: АТ «Кредобанк» повинен мати системи резервного копіювання та відновлення даних, щоб забезпечити можливість відновлення інформації в разі випадку втрати, пошкодження або крадіжки даних.

Виявлення об'єктів захисту :у результаті аналізу засобів, методів обробки інформації та переліку інформації, яка потребує захисту та циркулює в системі, можна виділити наступні об’єкти захисту. Також розглянемо (рисунок 1.1) структурна схема мережі на АТ «Кредобанк».

Приміщення для зберігання та обробки інформації, яка потребує захисту:

– ІТ-відділ;
– серверне приміщення.
– Сервери підприємства:
– веб-сервер;
– файловий сервер;

– сервер БД;
– поштовий сервер;
– контролер домена;
– АРМ робітників підприємства.

Інформаційна структура:
– ОС на АРМ;
– ПЗ на АРМ;
– Системи безперебійного живлення серверів та АРМ.

Персонал:
– Засоби вводу-виводу та відображення інформації;
– периферійні пристрої;
– телефонні лінії зв'язку;
– лінії охоронної та пожежної сигналізації;
– лінії локальної комп'ютерної мережі.

Носії інформації:
– паперові носії;
– флеш-накопичувачі.

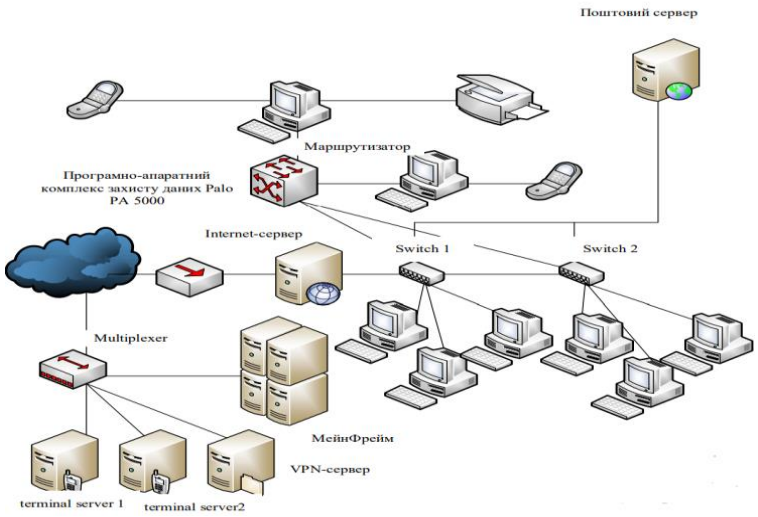


Рисунок 1.1 структурна схема мережі на АТ «Кредобанк»

1.4 Розробка моделі загроз і вразливостей виявлених об’єктів захисту на АТ «Кредобанк»

1. Стихійні лиха і аварії(може привести до повної втрати бази даних клієнтів «Кредобанку», тому бажано всі бази записати на носій пам`яті та сховати у внутрішньому сейфі).

– Збої і відмови устаткування(може привести до помилок розрахунків у програмі обробки рахунків вкладників та кредиторів);

– Помилки експлуатації(проведення інструктажів з техніки безпеки, інакше наслідки можуть бути такі ж, як і у вище описаних загрозах);

– Навмисні дії зловмисників і порушників(зловмисники можуть заволодіти цінною інформацією, такою, як реквізити вкладників, номери рахунків у «Кредобанк» у банках, логін та пароль користувача володіючи такою інформацією зловмисники можуть наважитися на пограбування як самих вкладників(адже будуть знати їх імена, суми вкладів та дату закінчення договору шляхом входу в систему через відомий логін-пароль та зміни даних договору(суми внеску, наприклад).

2. За природою виникнення:

– природні загрози;

– штучні загрози (загрози, що викликані діяльністю людини).

3. За принципом НСД:

– фізичний доступ - подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів(може призвести до втрати важливих документів);

– розкрадання документів і носіїв інформації(може призвести до втрати договору з вкладником(кредитором) через відсутність документальних підтверджень його вкладу(кредиту)).

4. Логічний доступ:

– доступ з використанням засобів комп'ютерної системи;

– порушення конфіденційності (розкриття інформації);

– порушення цілісності (повне або часткове знищення інформації, її спотворення, фальсифікація, дезінформація);

– порушення доступності (відмова в обслуговуванні).

5. За характером впливу:

– активні (в ході реалізації загрози вносяться зміни в систему);

– пасивний (спостереження).

6. За режимом НСД:

– при постійній участі людини (в інтерактивному режимі);

– можливе застосування стандартного ПЗ;– без особистої участі людини (у пакетному режимі), найчастіше для цього застосовується спеціалізоване ПЗ.

7. За типом (причиною появи) використовуваних вразливостей:

– недоліки політики безпеки;

– помилки адміністративного керування;

– недоліки алгоритмів захисту;

– помилки реалізації алгоритмів захисту

8. За способом впливу на об'єкт атаки:

– безпосередній вплив;

– вплив на систему дозволу.

9. За шляхом НСД:

– прямий стандартний шлях доступу;

– використання слабкостей політики безпеки;

– використання недоліків адміністративного керування;

– прихований нестандартний шлях доступу;

– недокументовані особливості системи, приховані канали.

10. За станом кінцевого об'єкта атаки:

– зберігання (як правило, об'єкт знаходиться на зовнішніх носіях);

– обробка (як правило, об'єкт знаходиться в оперативній пам'яті);

– передача (як правило, об'єкт знаходиться в лінії зв'язку) .

11. За наявністю зворотного зв'язку:

– із зворотним зв'язком (атакуючий отримує відповідь системи на його вплив);

– без зворотного зв'язку (атакуючий не отримує відповіді).

12. За рівнем моделі OSI, на якому здійснюється вплив:

– фізичний;

– канальний;

– мережний;

– транспортний;

– сеансовий.

Всі ці можливі загрози у фінансовій установі «Кредобанк» можуть призвести до втрати важливих фінансових документів, реквізитів вкладників(кредиторів), що саме по собі може призвести до великих грошових втрат, оприлюднення компрометуючої інформації, пограбування чи тиск на вкладників, що може призвести до статті кримінального кодексу «Злочинна халатність». Також ці загрози будуть онульовані при правильному розміщенні комп`ютера в приміщенні, при перевірці та докладному інструктажу персоналу, при недопусканні в приміщення бухгалтерії сторонніх людей, при повній професійності працівників серверної кімнати в цілому. Нижче переглянимо ймовірних категорій моделі порушника для АТ «Кредобанк» (таблиця 1.1-1.6).

Таблиця 1.1 Категорія порушників(Р)

Внутрішні	Рівень загрози
1	2
Співробітники підрозділів	3
Відвідувачі	1
Будь-які особи, що знаходяться за межами контрольованої зони	2

Кінець таблиці 1.1

1	2
Персонал, який обслуговує технічні засоби	2
Співробітники підрозділів супроводження програмного забезпечення	3
Хакери	3

Таблиця 1.2 Моделі порушника за мотивами здійснення порушень(M)

Мотив порушення	Рівень загрози
Безвідповідальність	1
Корисний інтерес	3
Професійний Обов'язок	4

Таблиця 1.3 Специфікація моделі порушника за рівнем кваліфікації та обізнаності (F)

Основні кваліфікаційні ознаки порушника	Рівень загрози
Володіє високим рівнем знань та практичними навичками роботи з технічними засобами	2
Знає недоліки та вади механізмів захисту, які вбудовано у системне програмне забезпечення та його недокументовані можливості	3
Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення	4

Таблиця 1.4 Специфікація моделі порушника за часом дії(T)

Характеристика можливостей порушника	Рівень загрози
1	2

Кінець таблиці 1.4

1	2
У робочий час	1
У неробочий час, під час планових перерв	2
Під час тимчасової зупинки системи	4

Таблиця 1.5 Специфікація моделі порушника за місцем дії (D)

Характеристика місця дії порушника	Рівень загрози
Без доступу на контрольовану територію	1
Усередині приміщень, але без доступу до технічних засобів	2
З доступом у зони даних	4
Робочі місця робітників	4

Таблиця 1.6 Профілі можливих порушників (P)

Категорія	Характер дій порушника				Рівень загроз
1	2	3	4	5	6
Порушники	m	f	t	d	Рівень загроз
Співробітники підрозділів	1,3	1	1,2	2,4	3
Відвідувачі	3	0	2	2,4	2
Будь-які особи, що знаходяться за межами контрольованої зони	3	1	3	1	2
Персонал, який обслуговує технічні засоби (інженери, техніки)	1,3	0	2,3	2	2
Співробітники підрозділів супроводження ПЗ	1,3	1,2,3	1,2,3	2,3,4	5

Кінець таблиці 1.6

1	2	3	4	5	6
Хакери	3	1,2	3	1,2	4

Результати розробки моделі загроз і вразливостей можуть служити основою для розробки стратегій безпеки, планів надзвичайних ситуацій та політик безпеки банку. Узагальнюючи, розробка моделі загроз і вразливостей виявлених об’єктів захисту на АТ "Кредобанк" допомагає банку аналізувати, розуміти та вирішувати питання, пов'язані з безпекою і захистом фінансових даних та інфраструктури. По результатам моделі загроз найбезпечнішими є : Співробітники підрозділів супроводження програмного забезпечення - найвищий бал загрози 5, наступний рівень це Хакери – 4 бали , та Співробітники підрозділів – 3 бали.

Також розглянемо (таблицю 1.7) писилаючись на інфорацію у цьому розділі а саме про модель порушника.

Таблиця 1.7 типові способи, засоби та категорії осіб, що здійснюють злочини у банківській сфері

Вид операцій	Основні способи здійснення злочинів	Засоби здійснення злочинів	Особи, які здійснюють злочини
1	2	3	4
Депозитні операції	Неправомірне проникнення в КСбанку. Підробка документів	Депозитні сертифікати. Комп’ютерні віруси. Помилкові комп’ютерні команди	В основному співробітники банку
Кредитні операції	Незаконне одержання кредиту. Не виплата	Надання позичальником підроблених	Особи, які не є співробітниками банку.

Кінець таблиці 1.7

1	2	3	4
	відсотків за кредитом. Навмисне неповернення кредиту	документів про кредитоспроможність або документів, що містять недостовірні дані. Фальсифікація надання застави	Співробітники банку у змові з третіми особами

2 РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ НА АТ «КРЕДОБАНК»

2.1 Політика інформаційної безпеки на АТ «Кредобанк»

Політика інформаційної безпеки АТ «Кредобанк» - це набір стратегій, процедур та практик, що визначає правила захисту інформації в банку та покликаний забезпечити безпеку даних клієнтів, захист від кіберзлочинності, забезпечення безпеки мережі та інших сфер діяльності банку, які пов'язані з інформацією. Політика інформаційної безпеки АТ "Кредобанк" має такі основні складові:

1. Організаційні заходи: організаційні заходи пов'язані зі створенням внутрішнього середовища, яке забезпечує безпеку інформації. Вони включають створення комітету з безпеки інформації, надання повноважень відповідальним особам за захист інформації, проведення перевірок безпеки інформації, навчання персоналу тощо. Ці заходи забезпечують ефективний контроль за доступом до інформації, а також забезпечують кваліфіковані знання з безпеки інформації.

2. Фізична безпека: фізична безпека пов'язана зі забезпеченням фізичного захисту приміщень, комп'ютерних систем, мереж та інших засобів зберігання і обробки інформації. До заходів фізичної безпеки можна віднести контроль доступу до приміщень, використання відеоспостереження, забезпечення безпеки обладнання тощо. Ці заходи допомагають зменшити ризик несанкціонованого доступу до інформації.

3. Технічна безпека: політика визначає правила забезпечення технічної безпеки, такі як захист мережі від несанкціонованого доступу, використання програмного забезпечення з відкритим вихідним кодом, використання ефективних методів шифрування, аудиту та моніторингу систем. До заходів фізичної безпеки можна віднести контроль доступу до приміщень, використання відеоспостереження, забезпечення безпеки обладнання тощо. Ці

заходи допомагають зменшити ризик несанкціонованого доступу до інформації.

4. Безпека даних: політика визначає правила забезпечення безпеки даних клієнтів та банку, такі як захист даних від несанкціонованого доступу, використання ефективних методів шифрування, забезпечення конфіденційності, цілісності та доступності даних. безпека пов'язана з захистом комп'ютерних систем, мереж та інших технічних засобів зберігання і обробки інформації від несанкціонованого доступу, зламів, вірусів тощо. До заходів технічної безпеки можна віднести: захист мережі, захист програмного забезпечення, використання файрвол.

5. Кадрова безпека: політика визначає правила забезпечення кадрової безпеки, такі як проведення перевірки на прийом нароботу, обмеження доступу до конфіденційної інформації, навчання персоналу з питань безпеки інформації. Навчання персоналу: всі працівники банку проходять навчання з питань інформаційної безпеки, що дозволяє підвищити рівень їх уважності та свідомості стосовно захисту конфіденційної інформації .Обмеження доступу до інформації: доступ до конфіденційної інформації надається лише тим працівникам, які мають на це відповідні повноваження. Проведення перевірок прийому на роботу.

6. Безпека зовнішніх сторін: політика визначає правила забезпечення безпеки взаємодії з зовнішніми сторонами, такі як постачальниками послуг, партнерами, клієнтами, захист від кібератак та інших загроз. Введення політики доступу, контролю і моніторингу віддаленого доступу до систем банку, включаючи віддалені канали комунікації та віртуальні приватні мережі. Прийняття заходів для захисту інформації, що передається через зовнішні мережі, зокрема шифруванням даних. Встановлення вимог до безпеки в контрактах з постачальниками послуг та виробниками програмного забезпечення.

7. Відповідальність: політика визначає відповідальність за забезпечення

безпеки інформації в банку, таку як визначення відповідальних осіб за захист інформації, проведення регулярних аудитів та оцінок ризиків, встановлення санкцій за порушення правил безпеки інформації. Призначення відповідальних осіб за забезпечення безпеки інформації в банку та налагодження системи контролю за дотриманням положень політики інформаційної безпеки. Розробка процедур і форм контролю відповідно до рівня ризику і потенційного впливу на безпеку інформації. Забезпечення належного навчання персоналу з питань безпеки інформації та встановлення системи стимулювання дотримання положень політики. Встановлення системи внутрішнього контролю та оцінки ефективності заходів забезпечення безпеки інформації.

Загальна мета Політики інформаційної безпеки АТ "Кредобанк" полягає в забезпеченні надійного захисту інформації від загроз, забезпеченні конфіденційності, цілісності та доступності даних клієнтів та банку, зниженні ризиків кібератак та інших загроз.

2.2 Апаратні та програмні засоби інформаційної безпеки на АТ “Кредобанк”

Обчислювальна система даної компанії є локальною мережею, яка складається з 13 комп'ютерів, що знаходяться в одному приміщенні Офіс знаходиться на одному поверсі будівлі. За генеральним планом у компанії 12 робочих кімнат. З яких12 кімнат - це робочі відділи компанії – 1 відділ це оператори , 2 відділ – юридичний , 3 відділ кадрів ,4 відділ – це бухгалтерія, 5 відділ – це кібербезпека, 6 відділ – це кімната із сервером та важливою документацією, 7 охоронець, та кабінет головного директора компанії АТ «Кредобанку» і приймальня працюють користувачі, це Windows Vista Business. Вибір цієї ОС оснований на тому, що дана версія Windows Vista спеціально розроблена для підприємств і має посилену політику безпеки і системи захисту.

Операційна система (ОС), що використовується на серверах компанії - Windows Server 2008 Standard Edition. Для забезпечення захисту ПК від НСД і несанкціонованого використання ІзОД приводи оптичних накопичувачів відімкнені у всіх комп'ютерах у підприємстві, крім комп'ютера головного директора і адміністраторів безпеки. При вході у систему на ПК завантажуються особисті дані з файлового сервера та сервера баз даних. При побудові плану розташування робочих місць ми керувались наступними принципами:· Екрани комп'ютерів не повинні бути повернуті до вікон або дверей. Робочі місця розміщені таким чином, щоб мінімізувати спостереження за роботою одних користувачів за іншими.

Характеристики фізичного середовища. Під час аналізу фізичного середовища потрібно також знайти та локалізувати можливі канали витоку інформації, що виходять за межу контрольованої зони. Це такі канали як: канали витоку інформації по ланцюгам електроживлення, канали витоку інформації по ланцюгам електроживлення, канали витоку інформації по ланцюгам заземлення, канали витоку інформації по вентиляційним системам. Територія компанії охороняється штатом охоронців у кількості 2 осіб. Крім того не ведеться відео нагляд за територією ,та в середині приміщення. У компанії не запроваджена система електронних пропусків, що збільшує імовірність загроз вчинити викрадення інформації зловмисником, що не є робітником фірми, не опосередковано з її території. Технічні характеристики каналів зв'язку. Для побудови локальної мережі використовується екранована вита пара. Згідно зі стандартами, для ізоляції мережевого кабелю, використовуємо екрановані металеві короба. В даного підприємстві обробляється відкрита та конфіденційна інформація. До конфіденційної інформації відносяться дані, що пов'язані з клієнтами фірми та їх справами, технологічна та ключова інформація. Нижче наведено приклад інформації що присутня на АТ «Кредобанк» та тип доступу до неї (таблиця 2.1).

Таблиця 2.1 Інформація та рівень доступу до неї

Назва	Тип доступу
База даних - клієнтів	конфіденційна
Договори	відкрита
Перелік обладнання	відкрита
База даних - працівників	конфіденційна
База даних засобів і ресурсів	конфіденційна
База даних телефонів клієнтів	конфіденційна
База даних телефонів працівників	відкрита
Партнери	відкрита
Журнал користувачів	відкрита
Журнал досягнень	відкрита

На підприємстві виконує роботу штат працівників чисельністю у 20 осіб для обслуговування громадян. Користувачі можуть використовувати систему для запису до черги на ту чи іншу послугу, надсилати електронні листи, мати доступ до персональних даних, використовуючи особистий кабінет, та також мати доступ до відкритої інформації. Для забезпечення роботи використовується набір сервісів:

– розподілена база даних;
– підсистема індексації та пошуку інформації;
– комунікаційна підсистема;
– підсистема адміністрування;
– підсистема захисту інформації.

Користувачі мають взаємодіяти із сервісами за допомогою клієнтського програмного забезпечення, системи прийому електронної пошти, програми доступу до даних, що розміщені у базі даних.

Програмно-апаратний комплекс включає наступні компоненти:

– сервери баз даних;
– сервери додатків;
– комунікаційні сервери;
– робочі місця адміністраторів й операторів;
– засоби резервування;
– периферійне обладнання, достатнє для ведення .

Програмне забезпечення. Для виконання більшості задач з програмного забезпечення загального призначення традиційно використовують офісні програмні продукти з пакету MS Office, розроблені для операційної системи Windows. Також використовують наступні програми:

– Mozilla - Internet-браузер (навігація в Internet та доступ до сервісів Internet);
– Oracle, MySQL - системи управління базами даних;
– Kaspersky Internet Security 2014 - антивірусна програма;
– 10-Strike LANState Pro - програма моніторингу серверів і комп'ютерів в мережі;
– Acronis Disk Director Home - управління розділами жорсткого диска;
– Auslogics BoostSpeed - оптимізація і прискорення роботи комп'ютера;
– Webitel – для дзвінків до клієнтів та внутрішнього звязку;
– 1с – програма у якій працюють як і оператори так і інші відділи;
– Корпоративна пошта outlook;
– Teams – чат у якомі знаходяться всі працівники ;
– Brookkeeper програма для обліку бухгалтера;
– Кадри плюс – програма для відділу кадрів ;
– Nmap, WinDirStat – програми для системного адміністратора;
– Microsoft office, exsel.

В результаті огляду місця працювання робітників було зафіксовано та

проаналізовано характеристику апаратних засобів що наведенна у (таблиці 2.2).

Таблиця 2.2 Апаратні засоби АТ «Кредобанку»

Найменування	Характеристики
Системний блок	Intel Core- i5 6500 KINGSTON -16 ГБ DDR4 RAM KINGSTON -256 ГБ SSD GeForce GTX 960 4GB
Монітор	Samsung 2243BW
Мишка	Logitech B100 USB Black
Клавіатура	Logitech K120
Сервер	Intel Xeon e 5410
Зовнішній	500гб
Маршрутизатор	TP-LINK TL-SG108

2.3 Комплекс програмно-апаратних засобів забезпечення інформаційної безпеки на АТ «Кредобанку»

Для гарантії того, щоб тільки зареєстровані в системі користувачі могли включити комп'ютер (завантажити операційну систему) та отримати доступ до його ресурсів, кожен доступ до даних у захищеній ос здійснюється у три етапи: ідентифікація – автентифікація – авторизація (рисунок 2.1).

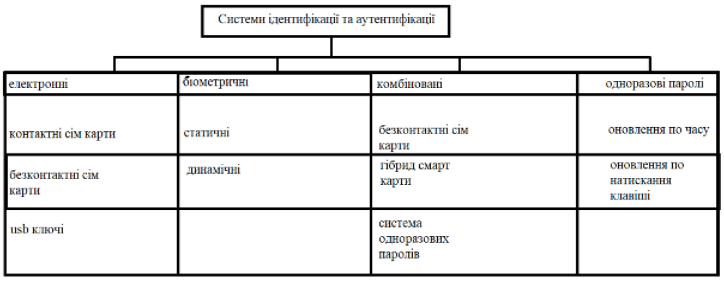


Рисунок 2.1 Класифікація програмно-апаратних систем ідентифікації та аутентифікації.

В електронних системах ідентифікаційні ознаки подаються у вигляді коду, що зберігається у пам'яті ідентифікатора (носія). Ідентифікатори у цьому випадку бувають такі: контактні смарт-картки; безконтактні смарт-картки; USB-ключі (USB-token); iButton. У біометричних системах ідентифікаційними є індивідуальні особливості людини, які у разі називаються біометричними ознаками. Ідентифікація виробляється з допомогою порівняння отриманих біометричних показників і які у основі шаблонів. Залежно від характеристик, що при цьому використовуються, біометричні системи діляться на статичні та динамічні. Статична біометрія ґрунтується на даних (шаблонах), отриманих з вимірювань анатомічних особливостей людини (відбитки пальців, візерунок райдужної оболонки ока і т.д.). Динамічна ґрунтується на аналізі дій людини (голос, параметри підпису, її динаміка. До складу електронних систем ідентифікації та аутентифікації входять контактні та безконтактні смарт-картки та USB-token. Безконтактні смарт-картки поділяються на ідентифікатори та смарт-картки, що базуються на міжнародних стандартах. В основі більшості пристроїв на базі безконтактних смарт-карток лежить технологія радіочастотної ідентифікації. Приклади характеристик безконтактних індифікаторів наведено у (таблиці 2.3) також нижче знаходиться схема із методами аунтифікації через смат-картку(рисунок 2.2).

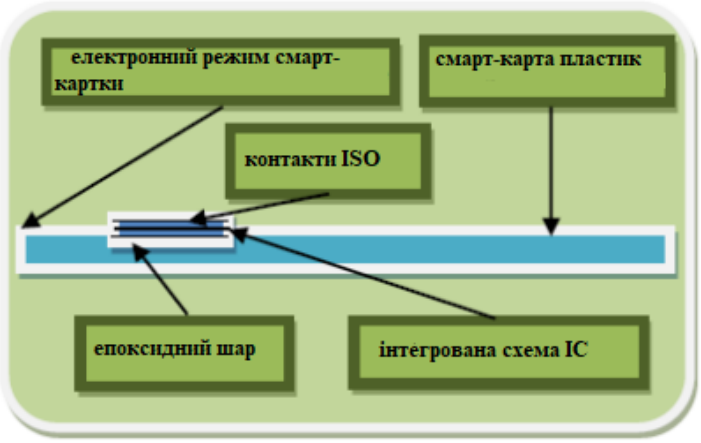


Рисунок 2.2 Схема дії смарт-карт

Таблиця 2.3 Характеристика індифікаторів

Характеристика	Proximity	Сім карти	
Назва	Proximity	ISO	IEC
Частота	125 кгц	13.56 мгц	13.56 мгц
Дистанція зчитування	До 1 м	До 10 см	До 1 м
Вбудовані типи чіпів	Мікросхема пам'яті, мікросхема із жорсткою логікою	Мікросхема пам'яті, мікросхема з жорсткою логікою, процесор	Мікросхема пам'яті, мікросхема із жорсткою логікою
Функція пам’яті	Тільки читання	Читання та запис	Читання та запис
Ємність пам’яті	8-256 байт	64 байт – 64 кбайт	256 байт – 2 кбайт
Алгоритми шифрування та аунтифікації	нема	Технологія MIRAGE,DES, 3DES,AES, RSA, ECC	DES, 3DES

Основними компонентами безконтактних пристроїв є чіп та антена. Ідентифікатори можуть бути активними (з батареями), так і пасивними (без джерела живлення). Ідентифікатори мають унікальні 32/64-розрядні серійні номери. Системи ідентифікації на базі Proximity не захищені криптографічно, за винятком спеціальних замовних систем.USB-ключі працюють із USB-портом комп'ютера. Виготовляються у вигляді брелоків. Кожен ключ має 32/64 розрядний серійний номер. Нижче перегянем характеристику usb-ключів у

(таблиці 2.4).

Таблиця 2.4 - характеристика usb- ключів

Ключі	Ємність пам’яті	Разрядність серійного номера	Алгоритми шифрования
iKey 20xx	8/32	64	DES (ECB и CBC), DESX, 3DES, RC2, RC5, MD5, RSA-1024/2048
eToken R2	16/32/64	32	DESX (ключ 120 біт), MD5
eToken Pro	16/32	32	RSA/1024, DES, 3DES, SHA-1
ePass 1000	8/32	64	MD5, MD5-HMAC
ePass 2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1

USB-ключі, представлені на ринку:eToken R2, eToken Pro – компанія Aladdin Knowledge Systems;iKey10xx, iKey20xx, iKey 3000 – компанія Rainbow Technologies;ePass 1000 ePass 2000 – фірма Feitian Technologies;

1. Хороше пз а саме Symantec Endpoint Protection 14.0. Основні характеристики: категорія організація, призначення - антивірус, система безпеки. Версія - Захист кінцевих точок Symantec 14. Захищені об'єкти - Робочий стіл, сервер, віртуальні машини.Основні переваги використання захисту кінцевих точок Symantec включають: проактивне сканування загроз – унікальна евристична технологія, яка блокує атаки нульового дня з мінімальною кількістю помилкових розпізнавань; Generic Exploit Block (нейтралізація спроб експлуатувати вразливості додатків);

– виявляє сигнатури відомих вразливостей з блокуванням коду навіть невідомих експлойтів;

– Raw Disk Scan - реалізує функцію для зчитування даних жорсткого диска;

Контроль пристроїв – контролює використання периферійних пристроїв та їх вплив на ПК. Модуль відповідає за ізоляцію периферійних пристроїв (зовнішньої флеш-пам'яті, принтерів, записувачів компакт-дисків, USB-пристроїв), щоб запобігти копіюванню до них конфіденційних даних;

Контроль додатків - при виявленні підозрілої активності додатків він блокує доступ до важливих процесів користувача, папок і файлів.

2. Робота та перевірка SSL- сертифікатів для запобігання втрати/витоку інформації в інтернеті:

Протокол включає два етапи взаємодії клієнта і сервера:

a) встановлення SSL - (процедура «рукостискання», від англ, «handshake»), на цьому етапі може проводитися аутентифікація сторін з'єднання, розподіл ключів сесії, визначаються настроюються параметри з'єднання;

b) захищене взаємодія використовуються наступні криптоалгоритми:

– асиметричні алгоритми RSA і Діффі-Хеллмана;

– алгоритми обчислення хеш-функцій MD5 і SHA1;

– алгоритми симетричного шифрування RC2, RC4, DES, Tri- pleDES, IDEA.У протоколі SSL v 3.0 і TLS перелік підтримуваних алгоритмів є розширюваним. Для підтвердження автентичності відкритих ключів використовуються цифрові сертифікати Протокол SSL дозволяє проводити наступні варіанти аутентифікації сторін взаємодії:

– аутентифікація сервера без аутентифікації клієнта (одностороння аутентифікація) - це найбільш часто використовуваний режим, що дозволяє встановити справжність сервера, але не проводить перевірки клієнта (адже подібна перевірка вимагає і від клієнта наявності сертифіката);

– взаємна аутентифікація сторін (перевіряється справжність як клієнта, так і сервера);

– відмова від аутентифікації - повна анонімність;

в даному випадку SSL забезпечує шифрування каналу і перевірку

цілісності, але не може захистити від атаки шляхом підміни учасників взаємодії

3. Криптографічне програмне забезпечення - це програми, що забезпечують шифрування і розшифрування даних для забезпечення конфіденційності інформації.

Шифрований пароль може бути розшифрований зловмисником, якщо він має доступ до зашифрованого пароля та ключа шифрування. Тому, для збереження паролів у більш безпечному форматі, рекомендується використовувати алгоритми хешування, такі як bcrypt, Алгоритми хешування забезпечують більш високий рівень безпеки, оскільки вони забезпечують невідновлюваний процес перетворення пароля в безпечний хеш, який не може бути розшифрований до початкового пароля. Крім того, для запобігання атакам типу dictionary або brute-force на пароль можна використовувати сіль (salt), яка додається до початкового пароля перед хешуванням. Приклад : приклад коду:

$password = "easypassword"; //простіший пароль, що вводиться користувачем

echo sha1($password); // Хеш такого пароля при обробці функцією sha1() будет таким :6c94d3b42518febd4ad747801d50a8972022f956

$salt = "f#@V)Hu^%Hgfds"; // використовуючи случайний набір символів, ми можемо змінити значенння хеша

echo sha1($salt . $password); // а вот хеш для пароля, доповненого сіллю: cd56a16759623378628c0d9336af69b74d9d71a5

Одним з рішень може бути створення унікальної солі для кожного користувача, щось на кшталт: $hash = sha1($user_id . $password);

Краще генерувати зовсім випадкову сіль, наприклад:

```
// генеруємо случайну стрічку довжиною в 22 символа
function unique_salt() {
    return substr(sha1(mt_rand()),0,22);
    }
$unique_salt = unique_salt();
```

$hash = sha1($unique_salt . $password); // формуємо хеш пароля.

Більш зручним варіантом уповільнення є використання алгоритму Blowfish, реалізованого в PHP через crypt(). Перевірити доступність цього алгоритму можна за допомогою if (CRYPT_BLOWFISH == 1) echo 'it works!'; PHP 5.3 Blowfish вже включений.

function myhash($password, $unique_salt) {

// сіль для blowfish має бути довжиною в 22 символа

 return crypt($password, '$2a10'.$unique_salt);

}

$2a — це вказівка на те, що використовуватиметься алгоритм Blowfish

$10 – це сила уповільнення функції. У разі дорівнює 2^10. Може набувати значень від 04 до 31

Використовуємо її на конкретному прикладі:

hash = '$2a$10$dfda807d832b094184faeu1elwhtR2Xhtuvs3R9J1nfRGBCudCCzC';

$password = "verysecret";

if (check_password($hash, $password)) {

   echo "Доступ дозволенний!";

} else {

   echo "Доступ закритий!";

}

function check_password($hash, $password) {

   // перші 29 символів хеша, включаючи алгоритм, «силу уповільнення» і оригінальну «сіль» помістим в перемінну $full_salt

   $full_salt = substr($hash, 0, 29);

   // виконаємо хеш-функцію для перемінної $password

   $new_hash = crypt($password, $full_salt);

   // повертаємо результат

(«істина» чи «брехня»)

return ($hash == $new_hash);

Такий код має забезпечити максимальну безпеку - підібрати пароль нормальної складності та довжини (програмними методами, звичайно) практично неможливо. Із наведенної інформації побудуємо схему ширування данних що зазначена на (рисунку 2.3).

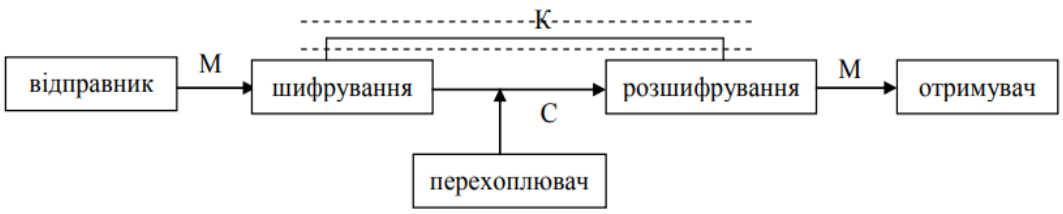


Рисунок 2.3 Схема шифрування данних

4. Використання захищеного внутрішнього приватного впн:

Використовувати захищений VPN - захищений віртуальний приватний мережевий з'єднання (VPN) може забезпечити додатковий рівень безпеки. Використання VPN забезпечує захист даних на рівні пристрою, що підключений до мережі, і може запобігти перехопленню чутливої інформації. Звичайне віртуальне приватне мережеве з'єднання (Virtual Private Network, VPN) - це мережа, яка забезпечує зв'язок між різними комп'ютерами чи пристроями через відкритий Інтернет. Захищений VPN (Secure VPN) використовується для забезпечення безпечного з'єднання між двома точками в мережі, яке забезпечує конфіденційність та цілісність даних, передаваних через мережу. Основною відмінністю між захищеним та звичайним VPN є те, що захищений VPN використовує криптографію та інші заходи безпеки для захисту переданих даних. Захищений VPN використовується для забезпечення безпеки віртуальної приватної мережі, яка може використовуватись для передачі конфіденційної інформації. Захищений VPN використовує протоколи, такі як SSL ,TLS та IPSec, для захисту переданих даних. Ці протоколи забезпечують криптографічний захист, що забезпечує конфіденційність даних, а також захист

від злочинних атак на мережу. Захищений VPN також може мати різні методи автентифікації та авторизації користувачів, що дозволяє обмежувати доступ до мережі для недозволених осіб. Крім того, захищений VPN може мати додаткові функції безпеки, такі як системи виявлення вторгнень (Intrusion Detection System, IDS) та виявлення вторгнень та запобігання їм (Intrusion Prevention System, IPS).Отже, відмінність між захищеним та звичайним VPN полягає в тому, що захищений VPN забезпечує безпеку за допомогою криптографії та інших заходів (рисунок 2.4).

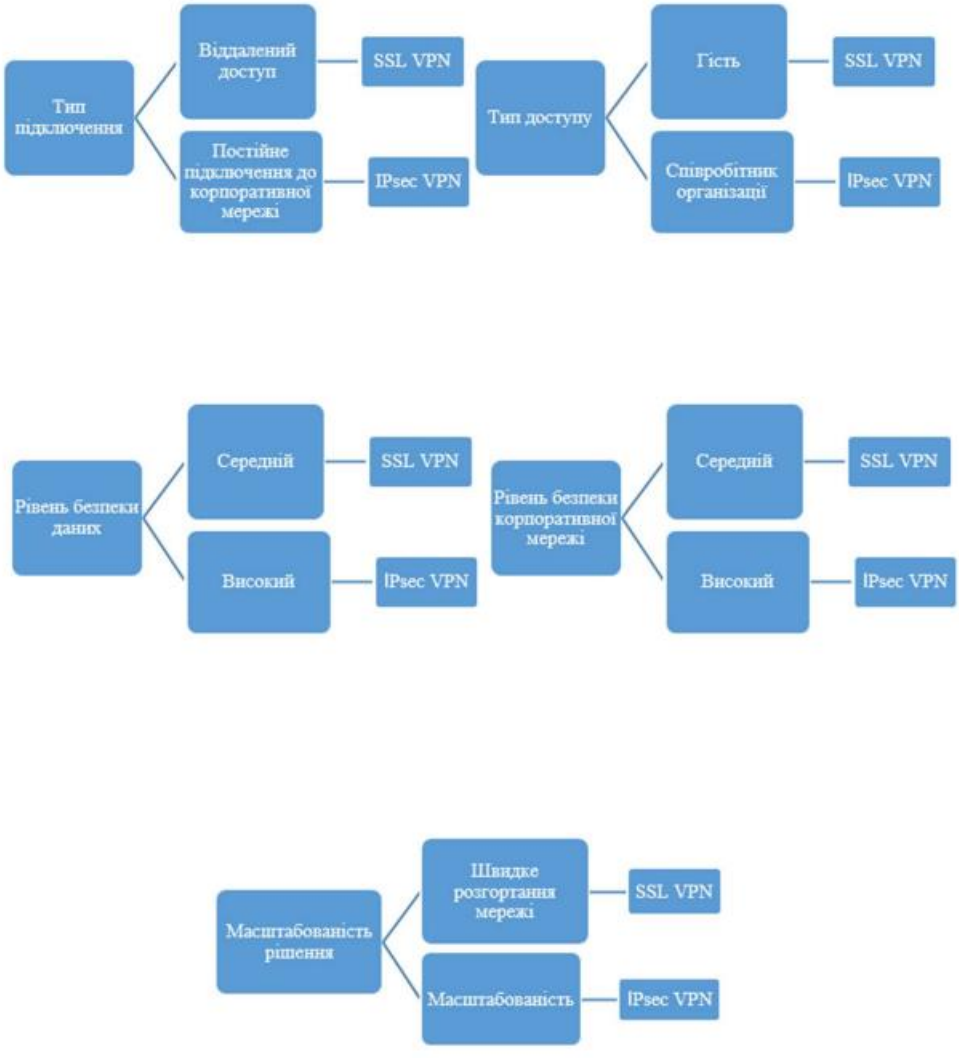


Рисунок 2.4 Порівняння захищеного vpn з різними сертифікатами

Процес аутентифікації імені користувача та пароля відбувається за

наступними етапами:

1. Користувач для входу в систему вводить логін та пароль, які відправляються на SSL VPN шлюз.

2. Аутентифікація користувача відбувається на AAA сервері, який отримує пароль та логін від SSL VPN шлюзу. Для авторизації лише сертифікатів не потрібно вводити логін і пароль. Сервер отримує сертифікат авторизації, обліку та аутентифікації від користувача. Дана авторизація відбувається в такій послідовності:

1. Користувач намагається отримати доступ до WebVPN за допомогою сертифікату аутентифікації AAA.

2. Шлюз WebVPN перевіряє клієнта за допомогою сертифікату автентифікації AAA, який був надісланий клієнтом. З'єднання не буде встановлено у випадку підтвердження недійсності сертифікату. В іншому випадку з'єднання успішно встановлюється.

3. Відбувається перевірка даних користувача на AAA сервері для підтвердження їх відповідності даним в сертифікаті. У комбінованій авторизації користувач вводить логін і пароль та надає сертифікат аутентифікації AAA. Даний процес відбувається наступним чином:

1. Здійснюється перевірка особи клієнта та сертифіката.

2. Для користувача відкривається сторінка авторизації

3. Користувач зазначає логін та пароль.

4. На AAA сервер надходить запит від WebVPN про аутентифікацію та авторизацію.

5. Далі списки користувачів, налаштовані на AAA, будуть використовуватись для авторизації та аутентифікації.

5.Фаєрвол:

Міжмережний екран (Firewall). Міжмережний екран (ME) – це спеціалізований комплекс міжм ережного захисту, який також називають брандмауером чи системою firewall. Зазвичай ME захищає внутрішню мережу

організації від «вторгнення» із глобальної мережі, також розглянемо побудову екрану розмежування доступу та зображення проксі-сервер із між мережевим екраном. Тоді він має розміщуватися між мережею, яку захищає, та потенційно ворожою мережею. Для більшості організацій МЕ є необхідною умовою забезпечення безпеки внутрішньої мережі. Можна класифікувати МЕ за такими ознаками. За функціонуванням на рівнях моделі OSI:

Пакетний фільтр (екрануючий маршрутизатор – screening router);

– Шлюз сеансового рівня (екрануючий транспорт);
– Прикладний шлюз (application gateway);
– Шлюз експертного рівня (statefull inspection firewall);

За виконанням:

– Апаратно-програмний;
– Програмний;
– Фільтрування трафіку;
– Фільтрування інформаційних потоків;

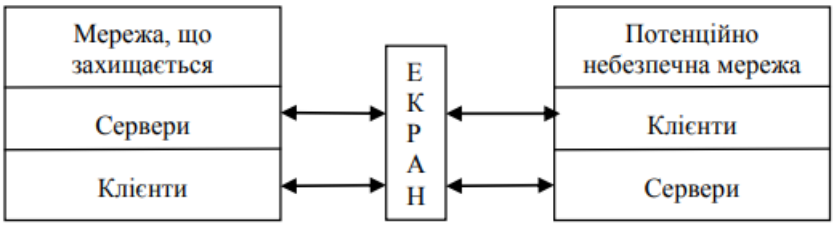


Рисунок 2.5 Екран як засіб розмежування доступу

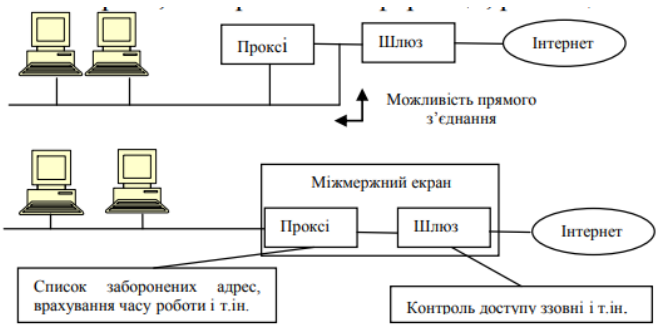


Рисунок 2.6 Проксі-сервер та міжмережний екран

При розгляді будь-якого питання, що стосується мережних технологій, основою служить еталонна модель ISO/OSI. Між мережеві екрани також доцільно класифікувати по тому, на якому рівні виробляється фільтрація канальному, мережному, транспортному чи прикладному. Відповідно, можна говорити про концентратори, що екранують, (рівень 2), маршрутизатори (рівень3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.

6. Двох факторна аунтифікація:

Two-Factor Authentication (2FA) — двохфакторна аутентифікація, підтвердження особи для отримання доступу до облікового запису, що забезпечує додатковий рівень захисту акаунту. Використовуючи 2FA, крім пароля треба ввести додатковий код з SMS або програми, включити розпізнавання голосу, залишити відбиток пальця тощо. Активація цієї функції ускладнює вхід до акаунту для сторонніх осіб. Крім того, важливою фічею є те, що ти отримуєш повідомлення, якщо хтось спробує це зробити замість тебе. Код 2FA є одноразовим, діє всього кілька секунд, хвилин або годин. Аутентифікація через СМС, дзвінок чи e-mail. На твій номер телефону здійснюється дзвінок або надходить повідомлення з кодом, який потрібно ввести в поле. Перевага цього способу полягає в тому, що отримати код можна без підключення до інтернету. Однак у разі втрати SIM-картки, телефону або в умовах поганої мережі ти вже не пройдеш аутентифікацію. Крім того, код може прийти на вказану зареєстровану пошту у вигляді комбінації символів чи як лінк. Схема типового підтвердження двохакторної аунтифікації зображена на (рисунку 2.7- рисунку 2.8).

– Аутентифікація за допомогою біометричних даних . Додатковим кодом для входу в обліковий запис у цьому випадку стає обличчя, голос, сітківка ока або відбиток пальця. Такий метод, як і використання спеціальних програм, забезпечує високий рівень захисту інформації, адже ніхто не зможе

скопіювати твої біометричні дані.

Рисунок 2.7 Двохфакторна аутентифікація

Рисунок 2.8 Схема аунтифікації через программу

7. Розмежування доступу:

Аналізуючи ризики для АТ «Кредобанку», що потребує захисту, які можуть виникнути в процесі її використання можна сформувати наступні правила розмежування доступу:

виконання правил розмежування доступу забезпечується застосуванням КЗЗ та організаційними заходами;

– усі особи, які беруть участь в обробленні ІзОД АТ «Кредобанку», повинні бути зареєстровані як користувачі АС;

– надання доступу до ІзОД здійснюється з урахуванням наданих згідно зі службовою необхідністю повноважень, за умови достовірного розпізнавання користувачів АТ «Кредобанку», встановленим КЗЗ. КЗЗ забезпечує можливість своєчасного доступу зареєстрованих користувачів АТ «Кредобанку», до ІзОД;

– кожний користувач АТ «Кредобанку», може мати носії ІзОД, які закріплені за ним персонально;

На підставі розглянутих у попередніх розділах моделей загроз та можливого порушника та враховуючи вимоги до політики безпеки та параметрів КСЗІ можна запропонувати наступну структуру КСЗІ на підприємстві, сфера діяльності якого – надання адміністративних послуг. Компоненти КСЗІ показані на рис. (таблиця 2.5),(рисунок 2.6).

Рисунок 2.9 Схема компонентів КЗСІ

Таблиця 2.5 Внутрішнє розмежування доступу

Технічні засоби системні і прикладне програмне забезпечення	Уповноважений персонал		
1	2	3	4

Кінець таблиці 2.5

1	2	3	4
Технічні засоби та ПЗ	Систем адмін	Відділ безпеки	Оператори
ОС серверів домену	-	Адмін права	-
ОС серверів системи управління мережним обладнанням захисту, за собі в управління,що встановлені	Адмін права	-	-
Програмні засоби захисту	Адмін права	Адмін права	-
Технологічна інформація поштового серверу, що встановлені на АРМ адміністрування активного мережного обладнання	Читання-модиф.	Читання	-
Мережні засоби захисту	Адмін права	Адмін права	-
Технологічна інформація серверів застосувань	Читання-модиф.	Читання-модиф.	-
Технологічна інформація серверів	Читання-модиф.	Читання-модиф.	-
Пошта	Читання-модиф.	Читання-модиф.	Читання-модиф.
Дані БД			Читання модиф.

КСЗІ в КРЕДОБАНКУ призначена для: забезпечення визначеної політики безпеки інформації, розмежування доступу користувачів інформації різних категорій конфіденційності, блокування несанкціонованих дій з ІзОД, реєстрації спроб реалізації загроз інформації та сповіщення адміністраторів безпеки про факти несанкціонованих дій з ІзОД, забезпечення спостереженості інформації шляхом контролю за діями користувачів та реєстрації подій, які мають відношення до безпеки інформації; підтримання цілісності критичних ресурсів; організації обліку, зберігання та обігу матеріальних носіїв інформації, забезпечення управління засобами захисту КСЗІ та контролю за її функціонуванням захисту ІзОД від її витоку технічними каналами.

2.4 Висновок

Висновок: Розробка політики інформаційної безпеки запобігання витоку та захисту інформації на АТ "Кредобанк" є критично важливим кроком у забезпеченні безпеки фінансових даних і довіри клієнтів. З метою забезпечення конфіденційності, цілісності та доступності інформації, банк повинен мати чітко визначену політику та строгі заходи безпеки, щоб запобігти витокам та захистити інформацію від несанкціонованого доступу. Розробка політики безпеки повинна включати аналіз потенційних загроз, визначення ризиків, розробку і впровадження заходів безпеки та моніторинг їх ефективності. Важливо враховувати всі аспекти безпеки, включаючи фізичну безпеку приміщень, мережеву безпеку, захист даних та захист від шахрайства. Політика інформаційної безпеки повинна бути чітко спрямована на всіх співробітників банку, починаючи від вищого рівня управління і до рядових працівників. Регулярне навчання та свідомість щодо інформаційної безпеки повинні бути основною частиною культури безпеки в організації. Також важливо встановити механізми виявлення і реагування на інциденти безпеки, а також забезпечити

резервне копіювання та відновлення даних. АТ "Кредобанк" повинен також дотримуватися всіх відповідних законодавчих норм та регуляторних вимог, пов'язаних з інформаційною безпекою, зокрема застосування стандартів.

3 РЕАЛІЗАЦІЯ РОБОТИ

3.1 Моделювання скуд та впровадження

На даний момент пропускна система реалізована частково за розробкою мого диплома бакалавра – низка автономних контролерів без додаткового живлення, сервер на базі операційної системи Linux Centos 7.0, контролери зчитувачів та електромеханічних замків Z-5R NET, безконтактні зчитувачі RFID-карток (браслетів, брелоків) Iron Logic Matrix-II, електромагнітні замки МЕТАКОМ ML -250 для блокування дверей та безконтактний USB зчитувач програматор RFID-карток Z-2 USB EM & HID PROX II & Mifare для програмування RFID-карток, під’єднаний до робочого комп’ютера завідувача з учбової частини, який виконує обов’язки адміністратора системи, а також турнікети Oxgard Praktika T-01. Поточна архітектура виглядає таким чином (рисунок 3.1).

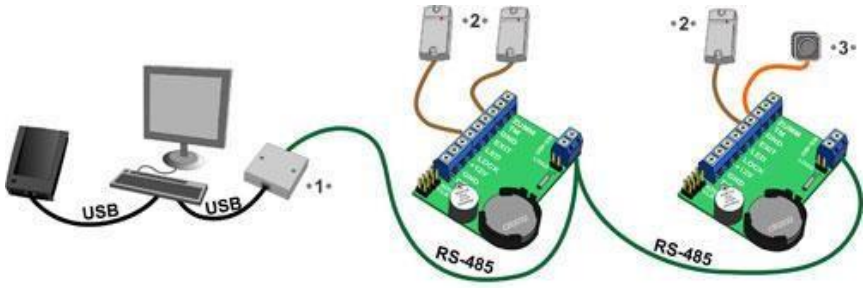


Рисунок 3.1 Архітектура

Кожному співробітнику або відвідувачу видається ідентифікатор (електронний ключ) – пластикову картку, яка містить в собі індивідуальний код. Ці «електронні ключі» видаються в результаті реєстрації перелічених осіб за допомогою засобів системи. Фото при наявності і відомості про власника «електронного ключа» заносяться в персональну «електронну картку». Персональна «електронна картка» власника і код його «електронного ключа» зв'язуються один з одним і заносяться в спеціально організовану комп'ютерну базу даних. Зараз зчитувач встановлено на

турнікеті біля вхідної двері. Вони зчитують з карток їх код та інформацію про права доступу власника карти і передають цю інформацію в контролер системи. У системі кожному коду поставлена у відповідність інформація про права власника картки. На основі зіставлення цієї інформації та ситуації, при якій була пред'явлена картка, система приймає рішення: контролер відкриває або блокує турнікет. Всі факти пред'явлення карток і пов'язані з ними дії (проходи, тривоги і т.д.) будуть фіксуватися в контролері і зберігатися в комп'ютері. Інформація про події, викликаних пред'явленням карток, може бути використана в подальшому для отримання звітів по обліку робочого часу, порушень дисципліни та інш. Структура системи контролю і управлінням доступу:

Як вже зазначалося вище, основним напрямком розвитку СКУД є їх інтелектуалізація, агрегування максимально можливої кількості функцій по збору, обробки інформації та прийняття рішень. Системи СКУД здатні автоматизувати безліч процесів, пов'язаних з організацією доступу до ресурсу. Сюди входять реєстрація суб'єктів (користувачів і персоналу) і об'єктів (ресурсів) СКУД, безпосереднє надання доступу до ресурсу, організація контролю роботи персоналу, збір і надання статистики щодо функціонування системи і багато іншого. В цілому систему можна поділити на дві підсистеми – апаратну та програмну. До апаратної підсистемі СКУД відносяться:

– зчитувачі (призначені для зчитування ідентифікаторів і передачі відповідної інформації в контролери);

– контролери (здійснюють обробку отриманої від зчитувачів інформації, приймають рішення про допуск або заборону проходу, передають інформацію на сервер системи);

– сервери (здійснюють накопичувати інформацію про всі проходи через БлП – час, дата, П.І.Б. та посада користувачів);

– комп'ютери з ПЗ (забезпечують моніторинг, централізоване

управління системою, ведення журналу подій, побудова звітів);

– виконавчі пристрої (в нашому випадку – електромеханічні замки та турнікети, які забезпечують блокування дверей і проходів);

– блоки живлення (забезпечують електроживлення пристроїв системи як від мережі, так і від автономних джерел живлення);

– інше обладнання (кнопки виходу – забезпечують розблокування виконавчих пристроїв при виході з котрольованої зони; дверні дотягувачі – забезпечують закриття дверей). Так як на сервері крім сервера баз даних буде знаходиться і web-сервер, то необхідно враховувати, що для його ефективної роботи необхідно щоб 42 машина мала достатньо системних ресурсів. Тобто сервер, на якому буде функціонувати дана система, повинен володіти досить потужною апаратною платформою. Особливо це стосується обсягу оперативної пам'яті і до частоти роботи центрального процесора. Дані будуть зберігатися в базі даних. А так як втрата цих даних може привести до значних наслідків, отже, на сервері. повинні бути передбачені апаратні засоби резервного копіювання цієї бази у вигляді реплікації БД на зовнішній сервер або зовнішній жорсткий диск. Апаратні засоби управління повинні забезпечувати прийом інформації від зчитувачів, обробку інформації та вироблення сигналів управління на виконавчі пристрої. В якості керуючого елемента в СКУД, що розроблюється, передбачається використовувати мікроконтролер. Мікроконтролер в СКУД повинен забезпечувати: – обмін інформацією по лінії зв'язку між контролерами і засобами централізованого управління; – збереження даних в пам'яті системи, при обриві ліній зв'язку із засобами централізованого управління, відключення живлення і при переході на резервне живлення; – контроль ліній зв'язку між контролерами і засобами централізованого управління. Протоколи обміну інформацією повинні забезпечувати необхідну стійкість, швидкість обміну інформацією, а також (при необхідності) (властивість, що характеризує здатність протистояти атакам з боку порушника, метою яких є нав'язування помилкового

повідомлення, підміна переданого повідомлення або зміна даних, що зберігаються) і захист інформації (для систем підвищеної та високої стійкості). Пристрій, що зчитує має забезпечувати:

– зчитування ідентифікаційного ознаки;
– перетворення введеної інформації в електричний сигнал;
– передачу інформації на контролер СКУД

Оскільки в якості ідентифікатора була обрана RFID карта, то зчитувальний пристрій повинен бути RFID сканером. СКУД, орієнтовані на обслуговування великої кількості клієнтів, зазвичай мають модульну структуру, що дозволяє організувати робочі місця для різних служб, що забезпечують ефективне функціонування системи. Модульна схема забезпечується за рахунок використання архітектури клієнт-сервер. кількість і функціональність модулів залежать від призначення системи і виробника. Модулі (службові додатки) взаємодіють з центральним сервером СКУД який виконує роль деякого диспетчера, який займається обробкою запити додатків і події контролерів, датчиків і інших виконавчих пристроїв. Нижче розглянемо схему на (рисунку 3.2).

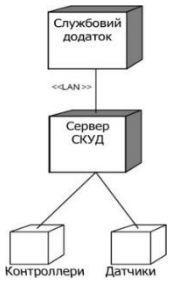


Рисунок 3.2 – Діаграма розгортання СКУД

Загальна схема системи, що проектується, виглядатиме наступним чином. (рисунок 3.3).В якості апаратної платформи було використано такі елементи системи:

– персональний комп’ютер для виконання ролі сервера бази даних, програмних модулів та обробки подій;

– контролери зчитувачів та електромеханічних замків Z-5R NET; безконтактні зчитувачі RFID-карток (браслетів, кілець тощо) Iron;

Рисунок 3.3 – Контролер електромагнітних замків та зчитувачів

Рисунок 3.4 – Безконтактний зчитувач RFID-карток

– безконтактний USB зчитувачі-програматор RFID-карток Z-2 USB EM & HID PROX II & Mifare для програмування RFID-карток для працівників;

– електромагнітні замки МЕТАКОМ ML-250 для блокування дверей. Нижче наведенно приклад одного із таких(рисунок 3.5)

Рисунок 3.5 – Безконтактний USB зчитувач-програматор RFID-карток

Рисунок 3.6 – Електромагнітний замок з дверним дотягувачем

– універсальний турнікет-тріпод півростовий Praktika–t–01 який може працювати як від пульту оператора (працівника служби охорони), так і під управлінням СКУД

Рисунок 3.7 – Турнікет Praktika–t–01

Турнікет має автоматичну функцію «Антипаніка» При виникненні тривожної ситуації – після натискання кнопки на пульті управління або за сигналом від пожежної сигналізації електропривод автоматично переводить планки в нижнє положення, повністю звільняючи прохід. Захист від зворотного провороту і утримання планок з вбудованою світловою та

звуковою сигналізацією запобігає несанкціоновані проходи «ланцюжком».

Рисунок 3.8 – Турнікет Praktika-t-01 в режимі «Антипаніка»

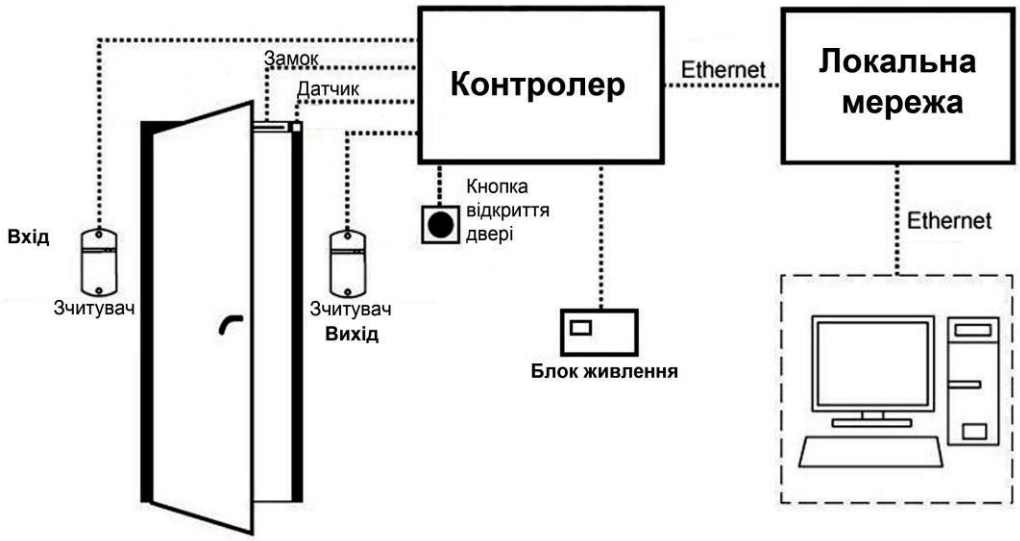


Рисунок 3.9 – Апаратна архітектура побудови СКУД

Програмні засоби реалізації: програмна платформа буде базуватись на сервері з операційною системою Linux Centos 8.0. Дана ОС підтримує практично всі панелі управління хостингами, тому не буде проблем налаштувати веб-сервер так, як це буде потрібне. Вона прекрасно настроюється, безпечна і стабільна, що теж важливо для додання їй цінності. Apache і Nginx – це два найпопулярніших веб-сервера в світі. Обидва використовуються для обробки HTTP-запитів, але кожен з них має власний

набір характеристик. В основі роботи веб-сервера Apache створення окремого процесу або потоку у відповідь на кожен користувальницький запит. Дана технологія досить легка в реалізації, але, на жаль, однозначно не підходить для проектів, у яких багато завдань. Будь-який процес «з'їдає» пам'ять і ресурси системи. Тому Apache підходить для сайтів з низьким рівнем завантаженості. В основі роботи веб-сервера Nginx – створення дочірніх процесів, які і обробляють запити. Тому дана технологія підходить більше для високонавантажених сайтів, які обслуговують тисячі з'єднань одночасно. За способом видачі контенту беб-сервер Apache генерує статичний і динамічний контент, тому його вибирають користувачі, які не мають бажання налаштовувати проксі і додаткові можливості для роботи з динамікою. На відміну від нього, Nginx видає тільки статичний контент, а ось динамічний не генерує. Правда, його можна використовувати в зв'язці з Apache, PHP-PFM або будь-яким іншим web-додатком, наприклад, Python (Django), Ruby on Rails, nodejs і т.і. Серед можливостей роботи з Apache слід виділити функцію конфігурації обробки запитів на рівні каталогів за допомогою прихованого файлу htaccess. За допомогою нього є можливість налаштувати авторизацію і аутентифікацію, кешування і права доступу користувачів. Конфігурацію міняти можна прямо під час роботи, при цьому не потрібно перезавантаження сервера і додаткова настройка сервера. Веб-сервер Nginx таких можливостей не має. Надається тільки один конфігураційний файл, який обробляє майстер. Для запуску оновлень конфігурації, необхідно відправити сигнал майстру і зробити перезавантаження сервера .На основі цього було зроблено вибір в бік веб-серверу Apache. Таким чином, було обрано майже стандартну серверну збірку LAMP – Linux, Apache, Mysql, PHP. LAMP – це абревіатура набору вільного ПЗ з від- критим кодом, в який входять ОС Linux, веб-сервер Apache, СУБД MySQL, та інтерпретатор Perl/PHP/Python – основні компоненти для побудови життєздатного багатоцільового веб-сервера. Також важливий момент – збірка веб-серверу буде здійснено з підтримкою SSL, та буде

придбано сертифікат безпеки від гідного центру сертифікації. Додатково розглянемо вибір мов програмування. Для створення програмного забезпечення під мікроконтролер існують різні мови програмування, але, мабуть, найбільш придатним є Сі, оскільки в цих мовах в найкращій мірі реалізовані всі необхідні можливості по управлінню апарат- ними засобами мікроконтролерів. С дозволяє створювати програми з набагато більшим комфортом, на- даючи розробнику всі переваги мови високого рівня. Компіляція вихідних текстів, написаних на С, здійснюється швидко і дає компактний, ефективний код. Основні переваги С перед асемблером:

– висока швидкість розробки програм;

– універсальність, яка не потребує досконального вивчення архітектури мікроконтролера;

– найкраща документовані і читаність алгоритму;

– наявність бібліотек функцій;

– підтримка обчислень з плаваючою точкою.

Розробка класів доступу: при розробці системи, було прийнято рішення використовувати ORM. ORM (абревіатура від Object Relational Mapping – Об'єктно реляційна проекція) – технологія програмування, яка зв'язує бази даних з концепціями об'єктно-орієнтованих мов програмування, створюючи «віртуальну об'єктну базу даних». Було розроблено ряд сутностей, які розглянемо нижче. «Рівень доступу» – дану сутність буде створено для обмеження або ж дозволу доступу тому чи іншому співробітнику в різні приміщення. «Група доступу» – сутність служитиме для об'єднання співробітників з однаковими правами доступу в одну підмножину. Для об'єднання персоналу буде створена дана сутність. «Доступні місця» – сутність вказує в які кімнати зможе входити люди- на, володіючи певними правами доступу. Ця сутність необхідна, так як, перш ніж пустити когось в приміщення, необхідно знати, чи має він на це право. «Користувач» – робочий персонал. Дана сутність зберігає персональні дані кожного

працівника хто має право доступу на територію та в окремі приміщення, «Пропущено через хворобу» – для обліку днів, проведених співробітниками лікарняному. За допомогою даної суті система може точно підрахувати яку суму заробітньої плати варто нарахувати співробітникам, з урахуванням лікарняних днів та скільки пропусків. «Реальна зарплата» – сума зароблених працівником грошей за місяць, з урахуванням лікарняних, преміальних і штрафних. «Переходи» – сутність для контролю і зберігання всіх переходів з одно- го приміщення в інше. Містить інформацію про час входу в приміщення, про місце від куди був здійснений перехід. Якщо співробітник вперше за день увійшов в цю кімнату, то в поле «від куди» буде зберігатися 0. Таким чином, можна відстежити, куди в першу чергу ходив співробітник. Так само сутність зберігає дані про проведений час в тому чи іншому приміщенні. «Кімната» – зберігає номер кабінету або приміщення і необхідний рівень доступу, для здійснення позитивного переходу. «Будівля» – сутність на випадок, коли приміщення розташовані на території більш ніж 1-го будинку. Під час проектування системи були створені діаграми класів, для спрощення розуміння «логіки» системи. Розглянемо набір класів, за допомогою яких забезпечується обмін даними між системою і базою даних. З верху перебуває інтерфейс IID, який розширюють все класи сутіності. Він створений для спрощення сприйняття коду програми. Для того що б не представляти всі класи у вигляді AbstractClass <ClassName, ID>, за допомогою даного інтерфейсу, ми представляємо класи як AbstractClass<ClassName>. Розглянемо кожну сутність окремо. Клас «AccessLevel» існує для зберігання рівня доступу до того чи іншого об'єкту для кожної групи персоналу. Клас «GroupWorker» необхідний для об'єднання персоналу в якесь безліч, за різними принципами, для забезпечення прав доступу. «WorkBench» зберігає дані про те, в яких приміщеннях працювати той чи інший співробітник. Це необхідно для того що б корректно підрахувати час проведений на робочому місці. Відсутність будь-якого з

приміщень в даному спис- ку вказує на те, що відповідна група користувачів не має права доступу до приміщення Клас «RealSalary», зберігає інформацію про заробітну плату за місяць, з урахуванням лікарняних, штрафних або ж преміальних. Клас «MissByIll» для ведення обліку про лікарняних кожного співробітника, ця інформація необхідна, для коректного підрахунку заробітної плати, за місяць. Клас «User» служить для зберігання і верифікації персональної інформації про співробітники підприємства. Використовуючи ці дані система приймає рішення щодо дозволу доступу в приміщення. Якщо співробітника з даними ID не існує в базі даних, то система заборонить доступ до будь-якому приміщенню. «Transition» необхідний для обліку інформації про переходах скоєних робочим персоналом. На основі цієї інформації будується список переходів певного співробітника, вираховується час проведений на робочому місці і розрахунок заробітної плати, а так само грунтуючись даною інформацією можна дізнатися де знаходитися працівник в даний момент. Нижче подано діаграму класів бізнес логіки системи контролю та управління доступом. Клас «Index» виступає в ролі головної сторінки системи, він створює об'єкт класу в якому започатковано всі необхідні компоненти розміщені на головній сторінці та проводиться розмітка сторінки. Так само клас «Index» відповідає за виклик всіх форм, усередині яких розміщена вся необхідна інформація для управління системою, на приклад форма «User» відображає список всіх користувачів з можливість фільтрувати список за різними критеріями. На формі «Stage» відображений план поверху, клікнувши на потрібну кімнату на плані приміщення відкривається список всіх співробітників знаходяться в цій кімнаті в даний момент. Так само можна знайти певного користувача на плані приміщення задавши його id або ж Прізвище та ініціали. Клас «AbstractForm» містить всі узагальнені методи всіх класів форм, такі як додавання, видалення, заміна, які відкривають користувачеві компоненти полів для введення даних. Кожна з форм займається відображенням даних на екран, а

так само їх додаванням, видаленням і заміною.

Реалізація структури бази даних: при побудові моделі даних в сукупність реквізитів об'єктів має відповідати вимогам нормалізації. Реквізити кожного об'єкта повинні відповідати вимогам, відповідним третій нормальній формі реляційної моделі даних. Виконання нормалізації забезпечує побудова реляційної БД без дублювання даних і можливість підтримки цілісності при внесенні змін. Аналізуючи мета створення БД системи контролю та управління доступом, є можливість відразу виділити об'єкт «Оператор», який матиме такі характеристики, наведені у (таблиці 3.1).

Таблиця 3.1 – Опис таблиці «Operator»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор групи користувачів
groupname	Varchar(255)	not null	Назва групи

– він має унікальний ідентифікатор – ключ;
– між описовими реквізитами немає функціональної залежності;
– кожен описовий реквізит функціонально залежить від ключа.

Тобто в отриманих об'єктах все описові реквізити логічно пов'язані. Також, в БД, що проектується, необхідно ввести ще дев'ять об'єктів: «Рівень доступу», «Робоче місце», «Користувач», «Пропущені через хворобу», «Зарплата», «Перехід», «Кімната», «Поверх» і «Будівля» описані нище.

Таблиця 3.2 – Опис таблиці «AccessLevel»

Назва	Тип даних	Обмеження	Опис
1	2	3	4

Кінець таблиці 3.2

1	2	3	4
Id	bigint(20)	not null	Первинний ключ
levelnumber	bigint(20)	not null	Рівень доступу до кімнати

Таблиця 3.3 – Опис таблиці «WorkBench»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифіка- тор групи робочого місця
workbenchNumber	bigint(20)	not null	Номер приміщення, робоче місце

Таблиця 3.4 – Опис таблиці «User»

Назва	Тип даних	Обмеження	Опис
1	2	3	4
id	bigint(20)	not null	Первиннийключ, ідентифіка-тор
FirstName	bigint(20)	not null	Им’я працівника
LastName	Varchar(255)	not null	Прізвище працівника
birthday	Date	not null	Дата народження
job	Varchar(255)	not null	Посада працівника
salary	Bigint(20)	not null	Ставка
address	Varchar(255)	not null	Домашня адреса
photo	Varchar(255)	not null	Шлях до фото на сервері

Кінець таблиці 3.4

1	2	3	4
departmentNam e	Varchar(255)	not null	Назва відділу
phone	Varchar(255)	not null	Телефон
obligedspendTi me	Bigin(20)	not null	Час присутності на місці
PassportData	Varchar(255)	not null	Серія и номер паспорту

Таблиця 3.5 – Опис таблиці «ReralSalary»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний іденти- фікатор заробітньої платні.
Date	Date	not null	Номер приміщення, що є робочим міс-цем
RealTimeWork	Bigint(20)	not null	Час перебування на робочому місці замісяць
Salary	Bigint(20)	not null	Нарахована зп лікарняних

Таблиця 3.6 – Опис таблиці «MissedByIllnes

Назва колонки	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ,
FromDate	Date	not null	Дата початку лікарняного
ToDate	Date	not null	Дата закінчення лікарняного

Таблиця 3.7 – Опис таблиці «Transition»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор переходу
fromRoom	Bigint(20)	not null	Номер приміщения
Io	Varchar(255)	not null	Час перебування на робочому місці за місяць
isAccessPermited	Tinyint(1)	not null	Нарахована заробітня платня з урахуванням премій, лікарняних та штрафів
Reason	Varchar	not null	Привід заборони доступу
spendTime	Bigint(20)	not null	Час перебування у приміщенні
timeIn	Date	not null	Час входу
Timeout	Date	not null	Час виходу
toRoom	Bigint(20)	not null	Номер приміщення, з якого виходимо

Таблиця 3.8 – Опис таблиці «Room»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор приміщення.
roomNumber	Int(11)	not null	Номер кімнати
acessLevel	Int(11)	not null	Рівень доступу

Таблиця 3.9 – Опис таблиці «Stage»

Назва	Тип даних	Обмеження	Опис
1	2	3	4
Id	bigint(20)	not null	Первинний ключ

Кінець таблиці 3.9

1	2	3	4
svgFilePath	Date	not null	Номер поверху
StageNumber	Not (11)	not null	Номер поверху

Таблиця 3.10 – Опис таблиці «Buildings»

Назва	Тип даних	Обмеження	Опис
Id	bigint(20)	not null	Первинний ключ, унікальний іденти- фікатор лікарняного
Address	Varchar(255)	not null	Дата початку лікарняного
buildingsNumber	Int(11)	not null	Дата закінчення лікарняного
svgFilePath	Varchar(255)	not null	Шлях до SVG файлу

Були виділені всі об'єкти предметної області, спираючись на фундаментальне базове поняття функціональних залежностей. Сукупність реквізитів об'єктів предметної області відповідає вимогам нормалізації. Зв'язки між об'єктами предметної області приведені в (таблиці 3.11). Були виділені всі об'єкти предметної області, спираючись на фундаментальне базове поняття функціональних залежностей. Сукупність реквізитів об'єктів предметної області відповідає вимогам нормалізації.

Таблиця 3.11 – Зв’язки об’єктів предметної області

Головний об’єкт	Підлеглий об’єкт	З’єднання	Ключ зв’язку
1	2	3	4
Група	Рівень доступу	1:M	Код_ групи
Група	Користувач	1:M	Код_ групи

Кінець таблиці 3.11

1	2	3	4
Група	Робоче	1:M	Код_ групи
Користувач	Зар. платня	1:M	Код_користувача
Користувач	Пропуск за хвороби	1:M	Код_користувача
Користувач	Перехід	1:M	Код_користувача
Перехід	Календар	M:1	Код_календара
Перехід	Кімната	M:1	Код_кімнати
Будівля	Поверх	1:M	Код_будівлі
Поверх	Кімната	1:M	Код_поверху

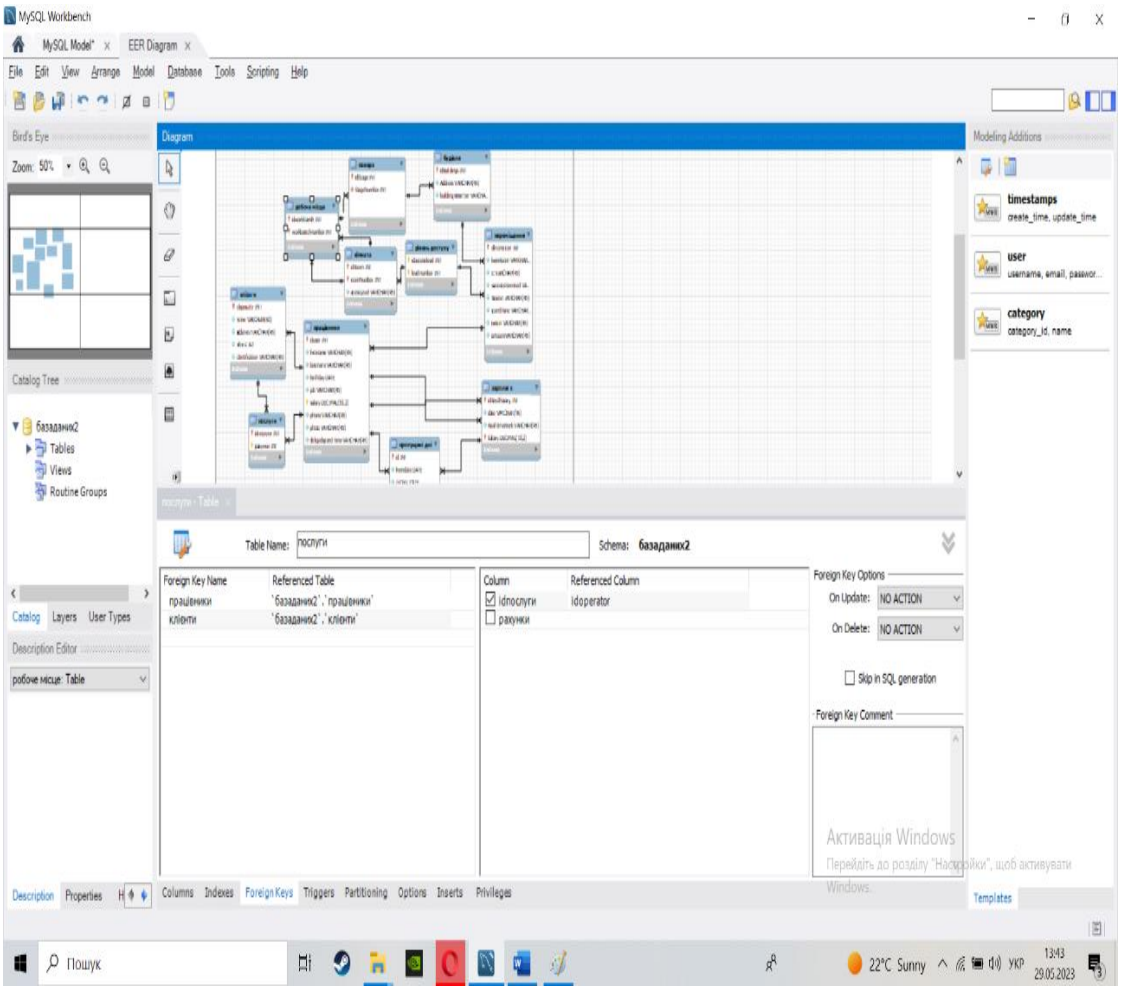


Рисунок 3.10 Схема бази даних

3.2 Розробка відеоспостереження на АТ «Кредобанк»

Які переваги Вам надасть система відеоспостереження: поліпшується продуктивність співробітників та якість обслуговування клієнтів. Безперервний контроль в реальному часі де б Ви не були: у відпустці, у відрядженні, на роботі. Встановлення відеоспостереження допомагає не тільки підтримувати високий рівень безпеки свого бізнесу, але і перешкоджає можливим порушення Контроль відвідувачів/чеків/черг та інша аналітика.

Зони огляду: КПП - мета спостереження у денному та нічному режимі ідентифікація особистості.

Головний коридор - ціль у спостереженні в денному та нічному режимі впізнання індифікація особистості, та перегляд за дотриманням нормового розпорядження.

Кабінет Бухгалтера, керівника, відділу безпеки, юр відділ та місце праці операторів - Спостереження ведеться лише у нічний час, або на запит бухгалтера чи керівника. Контролюються двері бухгалтера , відділу керівника , операторів ,юридичного відділу також прохідна охорони та відділ кадрів. Ціль спостереження ідентифікація особистості.

Вулиця - ціль спостереження в денному та нічному режимі: впізнання особистості та транспортного засобу, ніч – впізнання особистості та транспортного засобу. Завдання, що вирішуються:

1. Контроль несанкціонованого доступу співробітників та (або) порушників на територію об'єкта.

2. Контроль несанкціонованого доступу співробітників чи порушників на територію (або з території) об'єкта через огородження або заборонені зони.

3. Захист людей та матеріальних цінностей у межах контрольованої зони.

4. Ідентифікація особистості відвідувача чи співробітника під час проходження КПП, або за відвідуванні кабінету генерального директора.

5. Виявлення автомобілів, що в'їжджають на територію контрольованої

зони.

6. Автоматична фіксація та зберігання протягом певного часу запису протиправних чи інших подій з тривожного сповіщення з об'єкта, що захищається.

7. Виявлення та фіксування інших протиправних дій. Підреслюючи ці пункти нижче наведено приклад характеристики камер(таблиця 3.12) а також змодельована схема удосконалення відеоспостереження на АТ «Кредобанк»(рисунок 3.12).

Таблиця 3.12 Характеристика відеоспостереження

Назва	Пункт пропуску, вулиця	Бухгалтер, юр відділ, відділ безпеки	Директор
Розширення технологія	Hd HD-TVI	Hd AHD	Fullhd HD-CVI
Чутливість	0.2лк	0.2лк	0.2лк
Матриця і процессор	CMOS+ISP	CMOS+ISP	CMOS+ISP
Можливість одночасного підключення аналогових, HD та IP камер	-	+	+
Дальність передачі сигналу по кручений парі, м	+	150	150
WDR широкий динамический диапазон	Камера 6 мм кут огляду 44	Камера 2,8 мм кут огляду 110	Камера 2,8 мм має кут огляду 110
Сигнал	CVBS	CVBS	CVBS
Стандарт	Відкритий	Відкритий	Закритий
Передача звука по відеокабелю камер	Ні	Так	Так
Складність обслуговування	Низька	Середня	Середня
Ціна	Низька	Середня	Середня

Опираючись на інформацію описану вище розділом моделюємо архітектуру підключення відеоспостереження на АТ «Кродобанк» (рисунок 3.11).

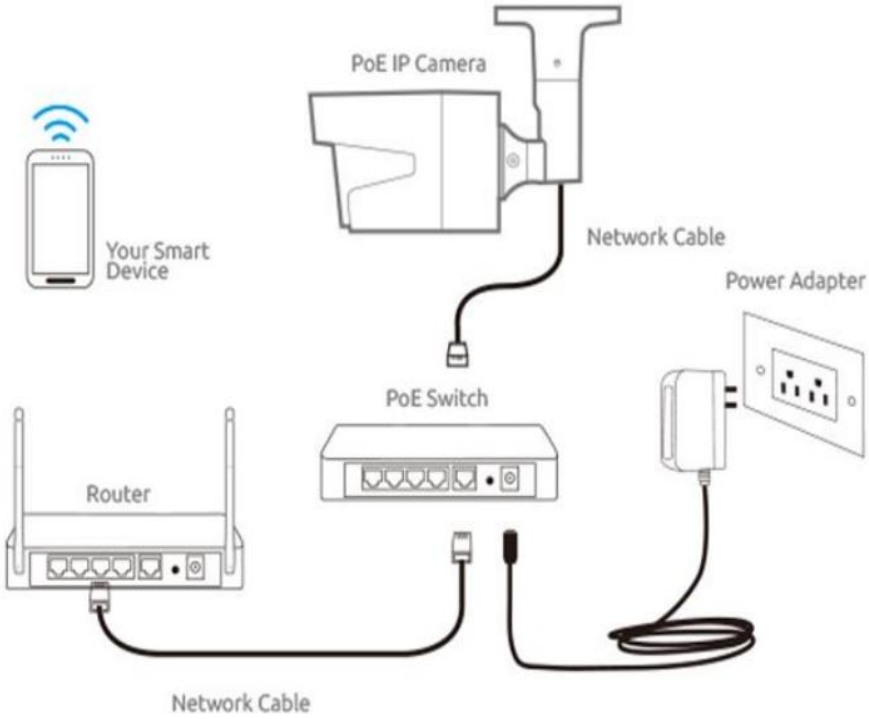


Рисунок 3.11 Метод підключення камер

Рисунок 3.12 схема приміщення з комп'ютерами та розміщення відеокамер вхідний контроль

Відеоспостереження - це система, яка використовує відеокамери для запису та перегляду подій, що відбуваються в конкретній області або приміщенні. Воно має безліч застосувань та вигод і здатне забезпечити безпеку, контроль і покращення ефективності в різних сферах. Ось кілька позитивних якостей відеоспостереження: Безпека: Однією з основних переваг відеоспостереження є забезпечення безпеки. Воно дозволяє контролювати та виявляти потенційні загрози або незаконні дії, такі як крадіжки, вандалізм, злочини чи неправомірні входження в приміщення. В разі виявлення подій охоронний персонал може вжити відповідних заходів для запобігання інцидентам або реагувати на них вчасно. Відстріл доказів: відеоспостереження забезпечує документацію та візуальні докази подій, що відбуваються. Це корисно в ситуаціях, коли потрібно з'ясувати, що сталося у певний час або встановити відповідальність за певні події. Відеозаписи можуть служити як важливі докази для правоохоронних органів, судових процесів або страхових справ. Контроль та моніторинг: відеоспостереження дозволяє здійснювати контроль та моніторинг важливих об'єктів, таких як банки, аеропорти, офісні приміщення, магазини тощо. Це допомагає управлінню та власникам моніторити дії персоналу, виявляти неефективність, встановлювати оптимальні робочі процедури та покращувати ефективність роботи. Запобігання злочинам: Відеоспостереження має відлякувальний ефект на потенційних злочинців. Люди, знаходячись під наглядом камер, схильні утримуватись від злочинних дій, оскільки свідомість про наявність відеозапису може спонукати до відповідальної поведінки. Таким чином, відеоспостереження сприяє створенню безпечніших середовищ та зменшенню рівня злочинності. Нагляд за дорожнім рухом: Системи відеоспостереження застосовуються для контролю та нагляду за дорожнім рухом. Вони можуть виявляти порушення правил дорожнього руху, небезпечні ситуації на дорозі, аварії та інші події, що впливають на безпеку на дорозі. Це допомагає забезпечити ефективний контроль над дорожнім рухом та допомагає в усуненні потенційних проблем.

3.3 Кошторис проетку.

Таблиця 3.13 Ціна проетку відеоспостереження

Місце	Назва	Ціна
Вулиця	Hikvision DS	800
Пункт пропуску	PTZ-120	1000
Бухгалтер	PRO VISION UKC KIT	3000
Юр відділ	PRO VISION UKC KIT	3000
Відділ безпеки	PRO VISION UKC KIT	3000
Директор	PRO VISION UKC KIT	3000
Рекрутер	PTZ-120	3000
Оператори	PRO VISION UKC KIT	3000
Охорона	Hikvision DS	3000
Всього		22800

Таблиця 3.14 Ціна проекту скуд для 2-х точок контролю

Назва	Ціна	Кількість	Сума
1	2	3	4
СКУД Parsec			
Контролер Parsec NC-000	11389	2	22778
Зчитувач PR-P09	7963	4	31852
ПК-інтерфейс Parsec NI-A01-USB	3338	2	6676
ПЗ базове PNWin-08	6667	1	6667
Програмний модуль обліку робочого часуз генератором звітів PNWin-AR	8272	1	8272
Програмний модуль підготовки, ведення бази даних пластикових карток PNWin-AR	13982	1	13982
Усього: за два пункти пропуску			90228
Усього у перерахунку один пункт проходу			45114

Кінець таблиці 3.14

1	2	3	4
СКУД Legos			
Контролер L5T04	11889	2	23778
Зчитувач PLR3	3193	4	12772
Конвертер CLE	4175	1	4175
ПЗ Люкс (32/3000)	18944	1	18944

ВИСНОВКИ

На основі проведеного дослідження та аналізу можна зробити висновок про те, що розроблена система комплексного забезпечення інформаційної безпеки щодо запобігання витоку та захисту конфіденційної інформації на АТ «Кредобанк» є ефективним інструментом для забезпечення безпеки інформаційних ресурсів банку. Дана система дозволяє виявляти, моніторити та протидіяти потенційним загрозам інформаційній безпеці, а також запобігати витоку конфіденційної інформації. Вона включає в себе комплекс заходів, таких як встановлення фізичного забезпечення, мережевої безпеки, криптографічного захисту даних, автентифікації та авторизації користувачів, а також проведення навчання та свідомості персоналу щодо інформаційної безпеки. Система комплексного забезпечення інформаційної безпеки на АТ «Кредобанк» є доречною, оскільки у сучасному світі інформаційні ризики зростають, атаки на банківські системи стають більш складними і винахідливими. Вона спроможна ефективно реагувати на нові загрози та вчасно виявляти вразливості в системі, що забезпечує надійний захист конфіденційної інформації клієнтів та операцій банку. Дана система також сприяє підвищенню репутації банку та довіри клієнтів, оскільки вона забезпечує конфіденційність, цілісність та доступність інформації, що є критичними факторами для успішної діяльності банку. Загалом, система комплексного забезпечення інформаційної безпеки на АТ "«Кредобанк» є важливим компонентом управління ризиками та забезпечення безпеки в сфері банківських послуг. Її ефективне функціонування є необхідним для збереження довіри клієнтів, захисту конфіденційної інформації та успішної роботи банку у сучасному інформаційному середовищі .В результаті виконаних робіт була створена гнучка архітектура системи контролю доступу, яка підтримує схему розрахунків користувачів за використання ресурсів. Реалізовано, за допомогою двигуна баз даних MySQL та мови PHP, були протестовані всі використовувані архітектурні механізми. Отримані наступні

результати:

– проведено системне дослідження предметної області. На його основі і на основі попередньої розробки була побудована відповідна модель;

– повністю перероблено, змодельовано, реалізовано і протестовано основні архітектурні механізми (взаємодія між всіма вбудованими об’єктами, інтеграція до системи сторонніх модулів та об’єктів, взаємодія клієнт-сервер за допомогою протоколу TCP/IP, параметризоване створення об'єктів, команди, механізми взаємодії додатків);

– розроблено архітектуру модулів програмного забезпечення і створені відповідні структурні моделі цих модулів;

– здійснено покращений захист даних, що могли бути втрачені завдяки шахраям, система працює під підписом та захистом сертифікату безпеки від надійного центру сертифікації. Практична цінність роботи полягає в наступному:

– розроблена архітектура модулів програмного забезпечення системи контролю доступу може бути і є використана в якості бази для побудови цілого ряду систем автоматизації систем контролю доступу бюджетного рівня, але досить надійного та гнучкого;

– створені механізми можуть бути повторно використані в будь-якому проекті, який висуває відповідні вимоги.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Техніко-економічна характеристика АТ “Кредобанк” [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://kredobank.com.ua/public/upload/2e6c391ae20109e86d5106ccbeaab99a.pdf.

2. АКЦІОНЕРНЕ ТОВАРИСТВО КРЕДОБАНКОКРЕМИЙ РІЧНИЙ ЗВІТЗА 2022 РІК [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступнона.

3. Статистичні дані [Електронний ресурс]:[Вебсайт]. – Режим доступу – Доступно на:https://kredobank.com.ua/about/zvity-banku/finansovi-zvity.

4. Політика інформаційної безпеки [Електронний ресурс]:[Вебсайт]. – Режим доступу – Доступно на: https://kredobank.com.ua/info/bank-security/polityka-informaciinoyi-bezpeky.

5. Витяг з Політики інформаційної безпеки [Електронний ресурс]: [Вебсайт] – Режим доступу – Доступно на:https://kredobank.com.ua/public/upload/62583e731db64e10b9c4deb6ba758fa5.pdf .

6. Повідомлення про порядок обробки і захист персональних даних [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://kredobank.com.ua/info/bank-security/personlni-dani/povidomlennya.

7. АНАЛІЗ І ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ БАНКІВСЬКИХ ТА КОМЕРЦІЙНИХ СИСТЕМ [Електронний ресурс] : [Вебсайт]. – Режим доступу – Доступно на:http://journals.dut.edu.ua/index.php/dataprotect/article/view/256.

8. Луцький М.Г. Дослідження програмних засобів аналізу та оцінки ризику інформаційної безпеки / Луцький М.Г., Корченко О.Г., Іванченко О.В., Казмірчук С.В. // Захист інформації - 2011. - №3. - С. 97-108.

9. Технічний захист інформації – Вікіпедія.

10. New Computerised Transit System (NCTS): Advantages to Companies. [Електронний ресурс].

11. Закон України "Про захист інформації в автоматизованих системах".

12. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. № 851-IV.

13. Чернишова, Н. В. Розробка моделей загроз і вразливостей інформаційних систем [Текст] / Н. В. Чернишова, В. А. Чернишов // Проблеми захисту інформації. - 2015. - № 2(34). - С. 59-64.

14. Карпенко, О. М. Розробка моделі загроз і вразливостей інформаційних систем на основі методу аналізу найбільш ймовірних атак [Текст] / О. М. Карпенко, І. М. Павленко // Вісник Харківського національного університету внутрішніх справ. - 2017. - № 4. - С. 157-165.

15. Модель порушника можливі шляхи і способи його проникнення на об`єкт, що охороняється [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://ua-referat.com/Модель_порушника_можливі_шляхи_і_способи_його_проникнення_на_об%60єкт,_що_охороняється.

16. Про захист інформації в інформаційно [Електронний ресурс] // Законодавство України. – 2014. – Режим доступу до ресурсу - Доступно на:https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

17.Хорев А.А. Технічний захист інформації: навч. посібник для студентів вищих навчальних закладів. У 3 т. т. 1. Масові викиди інформації. – М.: НВЦ «Аналітика», 2008. – 436 с.

18. Основи політики інформаційної безпеки для банків [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://www.bis.org/bcbs/publ/d436.htm.

19. Посібник із розробки політики інформаційної безпеки для фінансових установ [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://www.ffiec.gov/ffiecinfobase/booklets/information-security/1.

20. [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://www.sciencedirect.com/science/article/pii/S1877050915012867.

21. "Information Security: Principles and Practice" авторів Mark Stamp та Thomas A. Elmes - ця книга пропонує комплексний підхід до інформаційної безпеки, включаючи апаратні та програмні аспекти.

22. СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У ФІНАНСОВИХ УСТАНОВАХ [Електронний ресурс] [Вебсайт] – Режим доступу – Доступно на https://buklib.net/books/28521/.

23. Основи інформаційної безпеки. Навчальний посібник. — Вінниця: ВНТУ, 2009. — 268 с.

24. Методи і способи захисту інформації [Електронний ресурс] : [Вебсайт] – Режим доступу – Доступно на:https://pidru4niki.com/1801051351329/ekonomika/metodi_sposobi_zahistu_informatsiyi.

25. Бережнюк, М. І. Комплекс програмно-апаратних засобів забезпечення інформаційної безпеки [Електронний ресурс] / М. І. Бережнюк // Вісник Харківського національного університету внутрішніх справ. - 2017. - № 3. - С. 156-162. – Режим доступу:https://www.nbuv.gov.ua/old_jrn/natural/Vkhnuvs/2017_3/16bimvnp.pdf.

26. Миронов, О. А. Програмно-апаратний комплекс забезпечення інформаційної безпеки об'єктів критичної інфраструктури [Електронний ресурс] / О. А. Миронов, С. М. Курилов // Вісник Київського національного університету імені Тараса Шевченка. Серія: Радіотехніка, радіоапаратобудування. – 2019. - № 192. – С. 25-29. – Режим доступу: http://radio.kpi.ua/articles/issue/view/3924.

27. Кулик, В. М. Програмно-апаратний комплекс захисту інформаційної безпеки автоматизованої системи [Електронний ресурс] / В. М. Кулик, В. А. Ступницький // Системи управління, навігації та зв'язку. Збірник наукових праць. - 2017. - Вип. 3 (47). - С. 96-100. - Режим доступу:http://www.irbis-

nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/sunz_2017_3_25.pdf.

28. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

29. Кобильник К.О. Захист інформації в комп'ютеризованих системах [Електронний ресурс] 2013 - 30 с.

30. Access Control Systems: Security, Identity Management and Trust Models" (автор: Messaoud Benantar) [Електронний ресурс] - ця книга пропонує глибокий огляд систем контролю доступу, включаючи їх моделювання та впровадження.

31. "Security Engineering: A Guide to Building Dependable Distributed Systems" (автор: Ross J. Anderson) [Електронний ресурс].

32. "Design and Implementation of Access Control Systems" [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на: https://ieeexplore.ieee.org/document/6548904.

33. Положення про контроль за функціонуванням системи технічного захисту інформації.

34. Система контролю і управління доступом (СКУД) [Електронний ресурс]:[Вебсайт]. – Електронні дані. – Режим доступу – Доступно на:https://vistplus.com/it-poslugi/skud/.

35. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс]:[Вебсайт] – Електронні дані – Режим доступу:http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi.

36. Проектування системи відеоспостереження для внутрішнього та зовнішнього середовища [Електронний ресурс]:[Вебсайт] – Режим доступу – Доступно на:https://www.researchgate.net/publication/265256978_Video_Surveillance_Syste

m_Design_for_Indoor_and_Outdoor_Environments.

37. Bank Security Handbook" (Автор: G. K. Goodman)[Електронний ресурс] – Ця книга надає загальну інформацію про безпеку в банківській індустрії, включаючи розділи, присвячені відеоспостереженню .

38. Журнали та публікації, які спеціалізуються на області відеоспостереження, безпеки і банківських технологіях [Електронний ресурс] : [Вебсайт] – Режим доступу – Доступно на: https://securitytoday.com/Home.aspx.

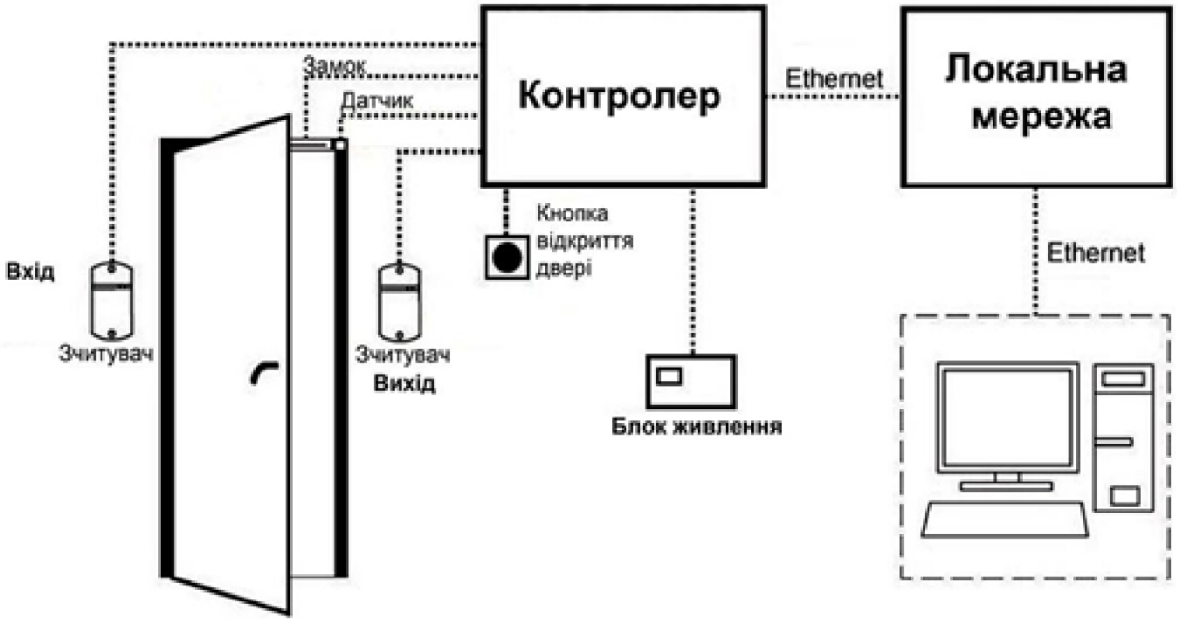
39. Design and Implementation of Intelligent Video Surveillance System Based on Deep Learning https://www.researchgate.net/publication/328086095_Design_and_Implementation_of_Intelligent_Video_Surveillance_System_Based_on_Deep_Learning.

40. Development of Video Surveillance Systems for Traffic Monitoring- https://www.sciencedirect.com/science/article/pii/S1877042815039619.

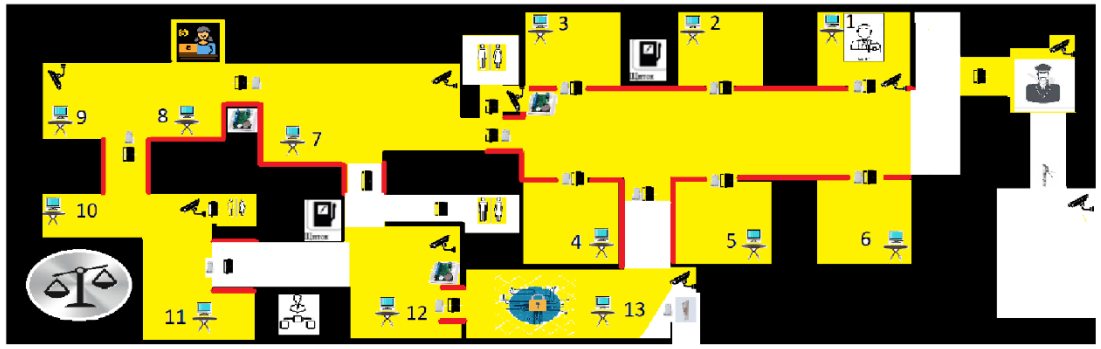
ДОДАТОК А

(обов’язковий)

Копія графічної частини



					КРКБ. 190101.19.01.02 ПЗ	
Зм.	Арк.	№ докум.	Підпис	Дата	Схема алгоритму спрацьовування антивірусу на небезпечне ПЗ	Літера / Маса / Масштаб
Розроб.		Вишковський Д. П.				
Перевір.		Джулій В.М				Аркуш 1 / Аркушів 3
Н.Контр.		Мостовий С.В				
Т.Контр.						ХНУ КБ-19-1
Затв.		Кльоц Ю.П.				



мережевий контролер

АРМ

Безконтактний зчитувач RFID-карток

Відділ обслуговування клієнтів

Охорона

Відділ кадрів

Головний турнікет

Додатковий турнікет вихід

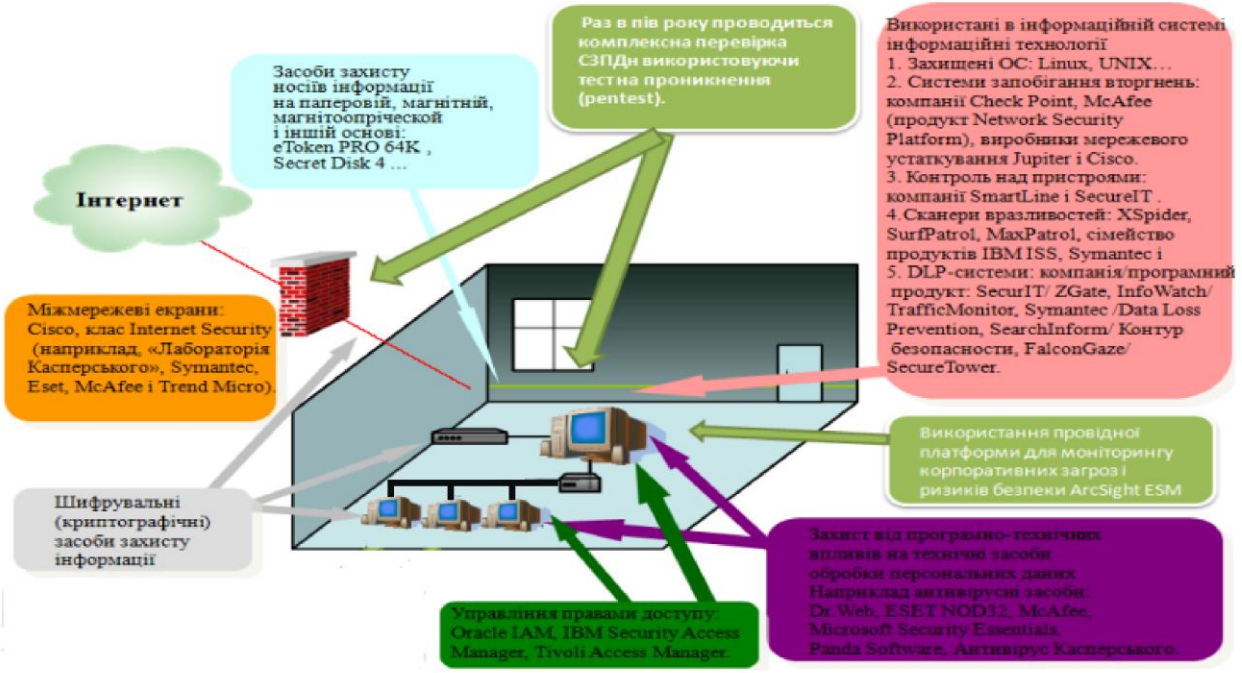
Відділ бухгалтерії

Юридичний відділ

Начальник

Відділ кібер безпеки

						КРКБ. 190101.19.01.02 ПЗ	
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Вишковський Д. П.			Схема алгоритму спрацьовування антивірусу на небезпечне ПЗ	Літера	Маса / Масштаб
Перевір.		Джулій В.М					
Н.Контр.		Мостовий С.В				Аркуш 2	Аркушів 3
Т.Контр.						ХНУ КБ-19-1	
Затв.		Кльоц Ю.П					



					КРКБ. 190101.19.01.02 ПЗ	
Зм.	Арк.	№ докум.	Підпис	Дата		
Розроб.		Вишковський Д. П.			Схема алгоритму спрацьовування антивірусу на небезпечне ПЗ	Літера / Маса / Масштаб
Перевір.		Джулій В.М				
Н.Контр.		Мостовий С.В				Аркуш 3 / Аркушів 3
Т.Контр.						
Затв.		Кльоц Ю.П				ХНУ КБ-19-1

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Вишковський Д.П

Тема: «Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ "Кредобанк"

Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3 ; кількість сторінок записки 68;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань та проблем комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ «Кредобанк». Для досягнення цієї мети було проведено дослідження різних засобів витоку інформації, та створено комплексну систему захисту інформації та впровадження її в дію в АТ «Кредобанк». Робота має на меті допомогти підприємствам забезпечити запобігання витоку інформації, легкість та простота використання нової комплексної системи захисту для співробітників в банку, та економічна ефективність у порівнянні з втратами що може зазнати банк у разі витоку захищеної конфіденційної інформації.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи та її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз систем захисту даних, що дозволило виявити проблеми та завдання, що потребують вирішення. У другому розділі було проаналізовано апаратні і програмні засоби інформаційної безпеки що використовувались в банку, створено політику інформаційної безпеки та комплекс програмно-апаратних засобі забезпечення інформаційної безпеки що дозволив реалізувати третю частину проекту . У третьому розділі головною задачею було моделювання та впровадження системи контролю управління доступу, розробка відеоспостереження та економічна ефективність . Проаналізувавши попередні розділи було створено КСЗІ.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, вона дозволяє розглянути розробку і впровадження системи комплексного захисту інформації, моделювання відеоспостереження та встановлення системи контролю управління доступу, що знижує ризик захисту конфіденційної інформації, захисту від вторгнень, покращення забезпечення цілісності даних, забезпечення безпеки мережі та захист від несанкціонованого доступу. Все це допомагає захистити конфіденційну інформацію підприємства, запобігає втратам даних та можливим кібератакам.. Підприємство зазнало покращення своєї інформаційної безпеки і здатне ефективно впоратися з потенційними загрозами і порушниками. В цілому, реалізація системи комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації виявилася успішним і відповідає вимогам та потребам підприємства. Застосування відповідних технологій та процедур дозволило забезпечити підвищену інформаційну безпеку і зменшити ризики несанкціонованого доступу. Реалізована система є надійною.

5. Негативні сторони проекту: кваліфікаційна робота в певних аспектах має недостатню кількість деталей або аналізу з питання комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації. Недостатня глибина аналізу може обмежити розуміння проблеми та можливість запропонувати належні рекомендації.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам.

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. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження Пункт апаратні та програмні засоби інформаційної безпеки та комплекс програмно-апаратних засобів забезпечення інформаційної безпеки могли б бути більш поглиблено розглянуті.

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «задовільно(D/3.50)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) _____
Гурман Іван Васильович, к.т.н., доцент кафедри інженерія програмного забезпечення Хмельницького національного університету

« _14_ » ____червня_____ 2023 . _____ (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Система комплексного забезпечення інформації щодо запобігання витоку та захисту конфіденційної інформації в АТ «Кредобанк»

Автор: Вишковський Денис Петрович
Спеціальність: 125 – Кібербезпека
Освітня програма: «Кібербезпека»
Науковий керівник: Джулій Володимир Миколайович, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Текст містить запозичення загальновживані фрази, цитати. До захисту допустити , але оцінку рекомендувати "задовільно".	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 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 допрацьована 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.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 78,3%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 70-100 %, визнається роботою з високою унікальністю тексту.

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

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 21.7%, з яких 3.97% є збігами з одним джерелом, збіги зумовленими наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.
2. Інші три збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань

Керівник роботи _____ В. М. Джулій

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015535820

Дата перевірки:
09.06.2023 16:48:12 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.06.2023 16:51:55 EEST

ID користувача:
100008300

Назва документа: Вишковський

Кількість сторінок: 72 Кількість слів: 13203 Кількість символів: 103321 Розмір файлу: 1.74 MB ID файлу: 1015188646

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

21.7%
Схожість

Найбільша схожість: 3.97% з Інтернет-джерелом (https://dut.edu.ua/uploads/p_421_17777559.pdf)

21.1% Джерела з Інтернету | 489 ..... Сторінка 74

2.98% Джерела з Бібліотеки | 151 ..... Сторінка 77

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 26

Підозріле форматування | 13 сторінок

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 115472 Назва: Система комплексного забезпечення інформаційної безпеки щодо запобігання витоку та захисту конфіденційної інформації на АТ "Кредобанк" Додано в БД: 2023-06-09 Автора: Вишковський Д.П. Керівники: Джулій В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	73745	1170	2632 (4%)	46 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми