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

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Забезпечення реалізації процесів попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації доступу до каналів передачі даних телекомунікаційної системи рекламного агентства
Назва теми

КвРКБ.170151.17.02.12 ПЗ
Шифр

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

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Назва

Виконав: студент IV курсу, група КБ–17–1 _____ Р.О. Пенцак
Підпис Ініціали, прізвище

Керівник _____ В.С. Орленко
Підпис, дата Ініціали, прізвище

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

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

« 01 » червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра кібербезпеки та комп'ютерних систем та мереж
Освітній рівень *бакалавр*
Галузь знань *12 «Інформаційні технології»*
Спеціальність *125 «Кібербезпека»*
Освітня програма *освітньо-професійна програма підготовки бакалавра*

ЗАТВЕРДЖУЮ:
Завідувач кафедри _____
_____
5 . 02 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Пенцаку Роману Олександровичу
Прізвище, ім'я, по батькові студента

1 Тема роботи «Забезпечення реалізації процесів попередження»
Керівник роботи Орленко В.С., к.т.н, доцент
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від ___ ____ 2021р. № ___
2 Строк подання студентом роботи на кафедру: _____
3 Вихідні дані до роботи методи попередження отриманню несанкціонованого доступу, авторизація доступу, системи аторизації доступу

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз об'єкта захисту, обгрунтування вибору засобів для побудови системи безпеки, проектування системи авторизації доступу на основі ролей, реалізація роботи

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
«Структура підприємства», «Модель загроз», «Інформаційні потоки підприємства», «Зв'язок бази даних з формами авторизації»

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
Нормоконтроль	Муляр І.В., доцент кафедри КбК СМ		
Антиплагіат	Муляр І.В., доцент кафедри КбК СМ		

7 Дата видачі завдання _____ _____ 2021 р.

КАЛЕНДАРНИЙ ПЛАН

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

Студент _____ Р.О. Пекуак
Підпис Ініціали, прізвище

Керівник роботи _____ Орленко В.С.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Забезпечення реалізації процесів попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації доступу до каналів передачі даних телекомунікаційної системи рекламного агентства».

Автор роботи: Пенцак Роман Олександрович.

Керівник роботи: Орленко Вікторія Сергіївна.

Обсяг – 57 с., 9 рис., 2 додатка, 11 джерел.

Графічна частина: 9 презентаційних слайдів, 4 плакати.

СИСТЕМА АВТОРИЗАЦІЇ ДОСТУПУ, ПОПЕРЕДЖЕННЯ ОТРИМАННЮ НЕСАНКЦІОНОВАНОГО ДОСТУПУ, НЕСАНКЦІОНОВАНИЙ ДОСТУП

Метою роботи є вивчення та аналіз проблеми протидії несанкціонованому доступу на етапі попередження, зокрема, за допомогою процесу авторизації, розробка та впровадження системи авторизації досутупу до каналів передачі даних телекомунікаційної системи рекламного агентства.

У роботі було проаналізовано та досліджено типові проблеми несанкціонованого доступу, особливу увагу було приділено питанню попередження отриманню несанкціонованого доступу та авторизації і контролю доступу на основі ролей.

В рамках кваліфікаційної роботи було розроблено систему авторизації доступу на основі ролей з використанням двофакторної автентифікації, під час проектування було враховано особливості діяльності підприємства.

Підпис студента

01.06.2021

Дата

Зона	Позиція	Позначення	Найменування	Кіл.	Прим.
	1		Завдання на дипломний проект	1	
	2		Анотація	1	
	3	КвРКБ.170151.17.01.12 ПЗ	Попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації Пояснювальна записка	1	
	4	КвРКБ.170151.17.01.12 Е8	Структура підприємства Схема структурна	1	
	5	КвРКБ.170151.17.01.12 Е8	Авторизація з 2FA Схема структурна	1	
	6	КвРКБ.170151.17.01.12 Е8	Модель загроз Схема структурна	1	
	7	КвРКБ.170151.17.01.12 Е8	Зв'язок бази даних з формами авторизації Схема структурна	1	

КвРКБ.170151.17.01.12 ВП

Арк.	№ Докум.	Підп.	Дата
Розробив	Пенцак Р.О.		
Перев.	Гітова В.Ю.		
Н. контр.	Муляр І.В.		
Зав.	Кльоц Ю.І.		

Попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації
Відомість проекту

Літера	Аркуш	Аркушів
н	1	1

ХНУ, КБ-17-1

ЗМІСТ

Зм.	Аркуш	№ докум.	Підпис	Дата	КвРКБ.170151.17.01.12 ПЗ		
Розробив		Пещак Р.О.			Попередження порушення несанкціонованого доступу та впровадження заходів по забезпеченню автентифікації. Пояснювальна записка	Літ.	Аркуш 2	Аркушів 70
Перевірив		Орленко В.С.						
Н.контр.		Мулик І.В.				ХНУ КБ-17-1		
Затвер.		Клюй Ю.П.						

ВСТУП

Будь-які важливі винаходи людства призводили не лише до спрощення на підвищення комфорту існування, а ще й до серйозних проблем, які раніше не можна було навіть уявити. Це стосується розвитку промисловості, транспорту, атомної енергетики і інформаційні технології не є вийнятком. Декілька десятків років тому, більшість людей і уявити не могли, що найближчим часом з'являться рішення, які дозволять спілкуватися та обмінюватися інфрмацією на відстанні в тисячі кілометрів, що всі сфери людського життя будуть настільки тісно пов'язані з інформаційними технлогіями.

Інформаційні технології значно спрощують життя в усіх сферах проте вище згадувалося про появи важливих проблем в зв'язку з серйозними винаходами. Зараз переважна більшість жителів цивілізованих країн мають можливість володіти персональним комп'ютером чи смартфоном, така поширенність інформаційних технлогій дає багато можливостей заробити проте не завжди законним шляхом. Такі можливості викликають зацікавленність у дуже широкого спектру щловмисників з різними інтересами та можливостями. Це породжує проблему інформаційної безпеки, адже без належної уваги питанням безпеки наслідки такого стрімкого розвитку технологій можуть бути катастрофічними.

Однією з загроз інформаційній безпеці є несанкціонований доступ. Несанціонованому досутуп можна протидіяти на декількох етапах, але в рамках кваліфікаційної роботи буде розглядатися саме етап попередження несанкціонованого доступу та один з методів попередження, а саме авторизація доступу.

Мета і завдання кваліфікаційної роботи. Метою є дослідження процесів попередження несанкціонованого доступу та авторизації доступу

до каналів передачі даних рекламного агентства з ціллю подальшого впровадження.

Завдання кваліфікаційної роботи:

- аналіз, систематизація, закріплення теоретичних знань і практичних умінь випускника, розвиток та закріплення навиків самостійної роботи;
- удосконалення вміння користуватись сучасними системами програмування, вирішувати інженерні задачі з проектування захищених інформаційних систем та їх елементів, використовуючи сучасні методології, інформаційні технології, здійснювати комп'ютерне моделювання, а також обробляти і систематизувати результати досліджень, використовуючи відповідні інструментальні засоби
- виявлення готовності до самостійної професійної діяльності.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Попередження несанкціонованого доступу

Несанкціонований доступ(НСД) до інформації – випадкове або навмисне отримання доступу до інформації особою, яка не володіє необхідними для цього повноваженнями, часто з ціллю порушення властивостей інформації та подальшим отриманням вигоди [1].

Наслідками НСД можуть бути:

- витік персональних даних співробітників, клієнтів, або партнерів;
- витік комерційної, банківської, державної чи інших видів таємниці, або інновацій та розробок;
- витік службової інформації;
- повна або часткова втрата працездатності системи безпеки, або підприємства в цілому.

Стрімкий розвиток інформаційних технологій веде за собою й розвиток зловмисників в цій галузі. В кіберзлочині може бути зацікавлена як звичайна кіберхуліган так і ціла держава(кібервійська). Тобто, інструментом для злодіяння може бути і звичайний персональний комп'ютер, і будь-які найновіші розробки, що створює величезний спектр загроз та методів їх реалізації.

Під способами несанкціонованого доступу до конфіденційної інформації прийнято розуміти різні методи, за допомогою яких зловмисник може отримати цінні дані організації, які є конфіденційними.

Для зручності представимо всі поширені способи у вигляді наступного переліку:

- Використання ініціативи з боку інсайдерів.
- Залучення до співпраці.
- Вивідування даних.

- Підслуховування.
- Таємне читання документів.
- Крадіжка даних.
- Несанкціоноване копіювання.
- Підробка.
- Підключення.
- Перехоплення.
- Фотографування.
- Часткове ознайомлення.
- Легальні методи.

Також окремо можна виділити знищення інформації, як серйозну загрозу діяльності організації. Розглянемо кожен з перерахованих способів докладніше.

Використання ініціативи

Зловмиснику неважко скористатися ініціативою співробітника, незадоволеного ситуацією, що склалася в організації. Практика показує, деякі співробітники або гостро потребують грошових коштах, або готові надати конфіденційну інформацію заради задоволення жадібності. Важливо розуміти, що використання ініціативи зловмисником ґрунтується не тільки на фінансовій мотивації. Нерідкісні випадки надання секретних відомостей заради помсти керівництву через образи [3].

Для отримання цінної інформації конкуренти можуть використовувати не тільки високопоставлених осіб або значущих фахівців, а й рядових співробітників.

Вербування співробітників

Вербування і підкуп співробітників-часто тривалий процес. Агенти конкуруючих фірм можуть місяцями збирати інформацію про працівника, членів його сім'ї. Це дозволяє знайти найбільш ефективний спосіб співпраці і зробити з такого співробітника власного агента, що працює в інтересах

конкуруючої фірми. Нерідко для схиляння інсайдера до співпраці збирають компрометуючі відомості, використовують погрози, психологічний вплив, грубі і агресивні методи залякування [3].

Також нерідкі випадки використання м'яких способів отримання засекречених даних. Зловмисники, прагнучи підступитися до фахівця, можуть працювати не безпосередньо, і передавати грошові кошти через сторонніх осіб і навіть відомих особистостей, що займаються громадською діяльністю.

Вивідування інформації

Способи вивідування інформації часто носять витончений характер. Поширена практика переманювання фахівців шляхом створення помилкових вакантних місць. Вакансія публікується для заманювання фахівця в пастку. Характерною особливістю такого прийому є обіцянка великих премій, пільг, високого рівня доходу. Вже на випробувальному терміні новачкові пропонують заробітну плату, що вдвічі перевищує його оклад в компанії конкурента. В ході співбесіди новачка приймають з обіймами і обіцяють добре винагороджувати за старання [3].

Багато фахівців з готовністю заковтують гачок і охоче демонструють «ноу-хау», діляться знаннями і досвідом, отриманими в своїй фірмі. Після закінчення випробувального терміну співробітнику дають відмову, отримавши від нього всю необхідну інформацію.

Інший спосіб вивідування інформації-спроба працевлаштування. Фірма конкурента відправляє свого агента з метою вивідування інформації, яку той отримує в ході співбесіди. Таким чином, можна дізнатися про поточні проблеми компанії, визначити "больові точки", дізнатися про використовувані стратегії і т. д.

Найефективніший метод вивідування інформації-спілкування з родичами, друзями, знайомими інсайдерів. У зв'язку з цим кожен співробітник, який має доступ до важливої інформації, повинен сформувати

правильну політику спілкування з оточенням і культуру поведінки в повсякденному житті.

Підслуховування

Підслуховування відноситься до найбільш популярних способів видобутку цінної інформації. Підслуховування здійснюється наступними методами:

- шляхом використання радіозакладок і мініатюрних диктофонів;
- шляхом використання програмного забезпечення для отримання значущих відомостей в ході телефонних переговорів, передачі радіосигналів;
- шляхом використання різної техніки, що вловлює (перехоплює) аудіосигнал.

Практикується також підслуховування при таємній присутності. Для попередження витоку інформації застосовуються пристрої, що заглушають передачу сигналу за рахунок створення радіоперешкод. Однак такі пристрої не допоможуть запобігти запис розмови на мініатюрний диктофон, який непомітно встановлюється в безпосередній близькості. Прилади, за допомогою яких виконується підслуховування, являють собою хитромудрі пристосування. Найчастіше зловмисники воліють проводити підслуховування в громадських місцях. Наприклад, кафетеріях. Підслуховуючий або записуючий розмову пристрій може бути легко закріплено на тілі і залишатися непомітним[3].

Спостереження

Спостереження за об'єктом дозволяє отримати багато цінних відомостей. Як і в разі підслуховування, даний спосіб передбачає застосування різних технічних пристосувань. Найпоширенішим пристроєм спостереження і стеження залишається фотоапарат.

Спостереження може вести як один, так і кілька людей. При груповому спостереженні один, рідше два спостерігача завжди знаходяться в безпосередній близькості і інформують іншу групу про поточну ситуацію. Даний спосіб використовують для з'ясування особливостей поведінки співробітника, маршрутів його пересування, іншої важливої інформації. Таким способом встановлюють факт підготовки організації до різного роду заходів [3].

Вести стеження можна як вдень, так і вночі. Сучасні системи дозволяють стежити за об'єктами при низькому рівні освітлення. Стеження можна виконувати на великих відстанях. Навіть в умовах практично повної темряви на відстані приблизно одного кілометра спостерігач легко зможе визначити потрібний об'єкт і впізнати людину.

Відстеження місця розташування об'єкта є важливою частиною стеження. Зазвичай для спрощення спостереження на об'єкт встановлюють радіомаяки. Якщо стеження ведеться за людиною, прилади закріплюють на його автомобілі.

Пристрої стеження відрізняються компактними розмірами і часто залишаються непомітними. Їх можна вмонтувати в фари автомобіля, замаскувати на деревах, на землі. Деякі прилади замасковані під предмети гардероба (ремені, капелюхи).

Розкрадання інформації

Найкращим способом запобігання крадіжки даних компанії є встановлення постійного контролю за співробітниками. Приблизно 80% людей не стануть красти важливі документи, оскільки це суперечить їх моралі. Використовуючи спокусу викрасти цінні відомості, можна убезпечити організацію від розкрадання конфіденційної інформації [3].

Копіювання даних

Копіювання інформації виконується різними способами, в тому числі за допомогою технічних засобів. Захист від копіювання електронної

інформації розроблена давно, проте зробити ксерокопію цінних документів здатний кожен співробітник організації. Тому необхідно встановлювати контроль за користуванням копіювальних апаратів [3].

Підробка і модифікація інформації

Підробити інформацію зловмисники можуть з метою отримання секретних даних. Підробці часто піддаються листи, рахунки, бухгалтерська документація.

Підробці і модифікуванню інформації передує промислове шпигунство, широко представлений в багатьох країнах світу. Один з видів підроблення даних являє собою пряму фальсифікацію, коли підробляються смс-повідомлення з метою отримання конфіденційних відомостей. Але найбільшого поширення в цьому відношенні отримали комп'ютерні віруси, здатні модифікувати програмне забезпечення для розкрадання документів та інформації [3].

Знищення та видалення даних (документів)

На сьогодні відомо чимало випадків застосування диверсійних методів, коли цінна інформація знищується (видаляється) будь-якими доступними способами. Знищення нерідко набуває кримінальний і навіть терористичний характер. Для видалення цінних відомостей можуть використовуватися спеціальні програми-віруси, звані «логічними бомбами». Так, в педагогічному центрі Ізраїлю (м.Хайфа) такий вірус знищив розробляється програмне забезпечення, на роботу з яким сумарно було витрачено більше 7 000 годин [3].

Підключення

Підключення виконується контактними і безконтактними методами. Зловмисники можуть підключитися з метою отримання інформації до лінії периферійних пристроїв великих і малих ЕОМ, лініях радіомовлення, лініях залів нарад, диспетчерських, лініях передачі даних. Можливо навіть підключення до ліній живлення і заземлення, оптоволоконних мереж [3].

Безконтактне підключення можна провести на величезній відстані від об'єкта. Для цієї мети можуть бути використані, наприклад, кільцеві Трансформатори.

Перехоплення інформації

Для перехоплення інформації можуть використовуватися наступні типи пристроїв:

- панорамні аналізатори;
- антенні підсилювачі широкосмугового типу;
- кінцева апаратура;
- антенні системи.

Ресивери можуть перехоплювати інформацію, поширювану за допомогою електромагнітних хвиль (наддовгі і короткі). Діапазон охоплення надзвичайно широкий. Сучасні засоби перехоплення дозволяють встановлювати радіоконтакт на відстані декількох десятків тисяч кілометрів. Небезпека перехоплення полягає в тому, що навіть без повної розшифровки отриманої інформації, зловмисники можуть зробити важливі висновки про діяльність організації.

Часткове ознайомлення з інформацією

Отримати доступ до інформації конфіденційного характеру часто виявляється неможливо. Однак навіть часткове ознайомлення з нею може задовольнити інтереси зловмисника. Випадковий або навмисно розкритий документ, що потрапив на очі відвідувачу, залишений включеним монітор з відображенням важливих відомостей-перелік ситуацій великий. Скористатися таким методом отримання інформації легко при частих порушеннях виробничої дисципліни в організації [3].

Для часткового ознайомлення можуть використовуватися і тонкі оптоволоконні кабелі з мікро-камерами. Такий кабель можна легко пропустити через замкову щілину.

Для часткового ознайомлення можуть використовуватися і тонкі оптоволоконні кабелі з мікро-камерами. Такий кабель можна легко пропустити через замкову щілину.

Особливо небезпечні особи, що володіють розвиненою зоровою(фотографічної) пам'яттю. Відомі випадки, коли агентам конкуруючих фірм для запам'ятовування важливих даних було достатньо тільки одного погляду на документи. Неодноразово такого роду крадіжці піддавалися лекала відомих дизайнерів і модельєрів, робочий процес яких бачили нібито випадкові відвідувачі. Важливо розуміти, що зловмисники з хорошою зоровою пам'яттю проходять спеціальні курси для швидкого вибудовування логічного ланцюжка і побудови висновків, що дозволяє їм не тільки запам'ятати цінні відомості, а й миттєво розкрити використовувані стратегії, плани [3].

Фотографування інформації

Отримання інформації шляхом фотографування дозволяє зловмисникам залишатися непомітними. В даний час існують об'єктиви і фотоапаратура, здатні робити знімки на відстані декількох сотень метрів і в результаті отримувати якісне зображення. Фотографування в інфрачервоному діапазоні дає можливість отримати дані з документами, в які були внесені виправлення і навіть відновити інформацію при читанні обгорілих документів. Фотокамера може бути вмонтована в годинник, замаскована під гаманець, запальничку, портсигар, а новітні пристрої виконуються у вигляді пластикових карт [3].

Легальні методи отримання конфіденційної інформації

Більшість компаній вважають за краще збір інформації легальними методами. Для цього співробітники можуть відвідувати різні офіційні заходи. Далі шляхом мозкового штурму і спільної роботи робити широкомасштабні висновки, що дозволяють розкрити важливі плани і стратегії конкурентів. Збір даних проводиться через торгових партнерів [2].

конкуруючої фірми, клієнтів, постачальників, підрядників, членів профспілок, практикантів. Тісні зв'язки з інформаційними виданнями та журналістами також допомагають добути цінні відомості.

Отже, таке різноманіття можливих загроз породжує масу методів та засобів захисту від загроз ІБ на різних етапах.

Протидія НСД складається з чотирьох етапів(рис. 1):

Рисунок 1.1 – Етапи протидії НСД

1) своєчасне виявлення загроз інформаційній безпеці;

2) локалізація, блокування та зупинення виявлених загроз;

3) ліквідація збитків, принесених загрозами, які не вдалось заблокувати;

4) аналіз відомих загроз та впровадження заходів, необхідних для їх уникнення.

В зв'язку з темою кваліфікаційної роботи нас цікавить саме етап попередження несанкціонованого доступу.

Організаційні заходи з попередження: періодичні оновлення політики безпеки і плану захисту, аналіз відомих загроз та прогнозування нових і дослідження відповідних методів захисту, постійні навчання та тренінги персоналу.

Інженерно-технічні заходи: контроль фізичних бар'єрів, а саме: паркану, дверей, вікон та гратів і штор/жалюзі на них; пломбування корпусів технічних засобів автоматизованої системи, використання систем екранування, зашумлення, заземлення, впровадження заходів авторизації та розмежування доступу.

1.2 Авторизація доступу

Авторизація-це механізм безпеки для визначення рівнів доступу або привілеїв користувача/клієнта, пов'язаних з системними ресурсами, включаючи файли, служби, комп'ютерні програми, дані та функції додатків. Це процес надання або відмови в доступі до мережевого ресурсу, який дозволяє користувачеві отримати доступ до різних ресурсів на основі особистості користувача [9].

Більшість систем веб-безпеки засновані на двоетапному процесі. Першим кроком є автентифікація, яка забезпечує ідентифікацію користувача, а другим етапом є авторизація, яка дозволяє користувачеві отримувати доступ до різних ресурсів на основі ідентифікації користувача. Сучасні операційні системи залежать від ефективно розроблених процесів авторизації для полегшення розгортання додатків і управління ними. Ключові фактори містять тип користувача, номер і облікові дані, що вимагають перевірки, а також відповідні дії і ролі [9].

Управління доступом в комп'ютерних системах і мережах ґрунтується на політиках доступу і ділиться на два етапи:

1) етап визначення політики, на якому дозволений доступ.

2) етап застосування політики, коли запити на доступ дозволені або не дозволені.

Таким чином, авторизація є функцією етапу визначення політики, який передує етапу застосування політики, коли запити на доступ дозволені або не дозволені на основі раніше визначених дозволів. Контроль доступу також використовує автентифікацію для перевірки особистості споживачів. Коли споживач намагається отримати доступ до ресурсу, процес контролю доступу перевіряє, чи був споживач уповноважений використовувати цей ресурс. Служби авторизації реалізуються сервером безпеки, який може контролювати доступ на рівні окремих файлів або програм.

1.2.1 Моделі і методи контролю доступу

Оскільки головна мета авторизації – обмеження та розмежування доступу користувачів до ресурсу, слід розглянути методи, якими ця мета досягається.

Мандатний контроль доступу (MAC)

Мандатний контроль доступу зазвичай вважається найбільш обмежувальним типом контролю доступу. Всі двері управляються налаштуваннями, створеними системними адміністраторами. У цій системі користувачі не можуть змінювати дозволи, що забороняють або дозволяють їм доступ в різні приміщення об'єкта, що забезпечує безпеку конфіденційних документів і даних. Система також обмежує здатність власника області або ресурсу забороняти або надавати доступ до ресурсів, перерахованих у файловій системі. Всі кінцеві користувачі класифікуються і забезпечуються ярликами, які дозволяють їм отримувати доступ тільки відповідно до встановлених правил безпеки. Наприклад, перевірка безпеки користувачів і класифікація даних (як конфіденційних, секретних або цілком секретних) використовуються в якості міток безпеки для визначення рівня довіри. Він обмежує доступ до ресурсів на основі чутливості

інформації, що міститься в ресурсі, і дозволу користувача на доступ до інформації з таким рівнем чутливості. Він зазвичай використовується державними органами та військовими через акцент на послідовну класифікацію та конфіденційність даних. Мандатний контроль доступу часто розглядається як протилежність наступному типу управління контролем доступу-дискреційному контролю доступу [9].

Дискреційний контроль доступу (DAC)

Дискреційний контроль доступу дозволяє власникам бізнесу вирішувати, хто може отримати доступ до яких областей приміщень або ресурсів. Власник даних має повний контроль над усіма програмами і файлами в своїй системі і визначає, хто може отримати доступ до певних ресурсів. Тому вони несуть відповідальність за вибір людей, які можуть увійти в певне місце, в цифровому або фізичному вигляді. Наприклад, системний адміністратор може створити ієрархію файлів для доступу на основі певних дозволів. Автентифікація користувача заснована на наданих облікових даних, таких як ім'я користувача та пароль. Цей тип управління доступом потім пропонує вибіркове обмеження, гарантуючи, що користувачі, які отримують доступ до системи, мають дозвіл на перегляд даних компанії [9].

DAC простий в реалізації і інтуїтивно зрозумілий, але може бути не найкращою системою через деякі її недоліків. Один з недоліків полягає в тому, що кінцевий користувач має повний контроль над налаштуваннями рівня безпеки для інших користувачів, що обмежує негативний контроль авторизації. Крім того, ця система вимагає більш активного управління для відкликання та надання дозволів, ніж жорстка система. DAC часто розглядається як протилежність своєму більш структурованому і жорсткому аналогу, MAC.

Управління доступом на основі ролей (RBAC)

Управління доступом на основі ролей призначене для дозволу або обмеження доступу на основі конкретних ролей з викладеними бізнес-обов'язками, а не окремого користувача. Роль співробітника в організації визначає дозволи, які йому надаються, і гарантує, що співробітники нижчого рівня не зможуть отримати доступ до конфіденційної інформації або виконувати завдання високого рівня. RBAC-найбільш поширена форма управління дозволами користувачів. Цей метод розроблений з використанням прав доступу, заснованих на змінних атрибутах, таких як потреби в ресурсах, завдання, середовище, місце розташування і багато іншого . Це спрощує для власників управління користувачами в групах на основі їх ролі або посади, а не призначення дозволів кожній конкретній особі. RBAC значною мірою виключає розсуд при наданні доступу до об'єктів. Наприклад, Спеціаліст з персоналу не повинен мати дозволів на створення мережевих облікових записів; ця роль повинна бути зарезервована для мережевих адміністраторів. Компанії значною мірою залежать від цієї моделі для захисту своїх конфіденційних даних і критично важливих додатків, підвищення операційної ефективності, підвищення відповідності вимогам, надання адміністраторам більшої видимості, зниження витрат і зниження ризику порушень і витоку даних. Безпека на основі ролей-це гнучкий і безпечний метод управління дозволами користувачів [9].

Управління доступом на основі правил

У цьому типі управління системою дозволу доступу засновані на структурованих правилах і політиках. Цей метод в значній мірі заснований на контексті, коли доступ надається або заборонений на основі набору правил, визначених системним адміністратором. Коли обліковий запис або група намагається отримати доступ до ресурсу, операційна система

перевіряє правила, що містяться в списку управління доступом для цього об'єкт [9].

Хоча доступ до управління на основі правил простий для розуміння, він часто поєднується з управлінням доступом на основі ролей для кращого застосування процедур і політик. Наприклад, класифікуючи роль і правила, він дозволяє адміністраторам встановлювати дозволи, що дозволяють студентам відвідувати лабораторію в певний час дня.

Управління доступом на основі атрибутів

Цей тип управління також відомий як управління на основі політики, оскільки він забезпечує різний динамічний і інтелектуальний контроль ризиків на основі конкретних атрибутів користувача. Атрибути використовуються в якості будівельних блоків, що описують запити доступу і визначають управління доступом. Потім політики набору можуть використовувати будь-який з цих атрибутів: атрибути об'єкта, атрибути ресурсу, атрибути середовища або атрибути користувача, щоб визначити, чи повинен користувач мати доступ [9].

Незважаючи на те, що він натхненний управлінням доступом на основі ролей, це просунутий спосіб визначення доступу з використанням таких атрибутів, як група, відділ, статус співробітника, громадянство, Посада, тип пристрою, IP-адреса або будь-які інші фактори. Ці атрибути також можуть бути отримані та імпортовані з бази даних, Salesforce, сервера LDAP або навіть від ділового партнера, що допомагає IT – відділу працювати з більшими бізнес-функціями.

Управління доступом на основі ідентифікації (IBAC)

IBAC-це спрощений метод забезпечення безпеки, який визначає, дозволено або заборонено використання людиною даного електронного ресурсу на основі його індивідуальної візуальної або біометричної особистості. Таким чином, користувачеві буде дозволено або заборонений доступ до електронного ресурсу в залежності від того, чи може його

особистість збігатися з ім'ям, яке з'являється в списку контролю доступу. Використовуючи це, мережеві адміністратори можуть більш ефективно управляти активністю і доступом в залежності від індивідуальних потреб. Деякі з переваг підходу до забезпечення безпеки, заснованого на ідентифікації особистості, включають в себе можливість здійснювати дуже чіткий контроль над тим, які служби і які функції можуть використовувати ці люди і які функції вони активно виконують. Крім того, є перевага в тому, що ви можете застосовувати політику контролю доступу на різних пристроях, таких як смартфони, планшети і ПК [9].

Управління доступом на основі історії (HBAC)

Рішення, прийняті цією системою управління контролем доступу, в основному засновані на минулих діях щодо забезпечення безпеки. Історичні дії користувача визначають, чи буде йому надано доступ чи ні. Це вимагає оцінки в режимі реального часу історії дій користувача, таких як час між запитами, зміст запитів, які двері були недавно відкриті і т.д. наприклад, доступ до певної службі або джерела даних може бути наданий або відхилений залежно від поведінки користувача в минулому, наприклад, інтервал запиту перевищує один запит в секунду [9].

Управління доступом на основі організації (OBAC)

OBAC допомагає при оцінці політик безпеки і дозволів більших організацій з декількома користувачами, таких як сторонні компанії. Цей метод забезпечує високий ступінь масштабованості і виразності. Кожна політика безпеки визначається організацією в рамках більшої системи і для неї. Таким чином, специфікація політики безпеки повністю параметризується організацією, щоб можна було одночасно обробляти кілька політик безпеки, пов'язаних з різними організаціями [9].

Контроль доступу на основы відповідальності

Системи, засновані на відповідальності, обмежують вхід або доступ в залежності від їх обов'язків в організації. Співробітники можуть отримувати

доступ тільки до інформації, необхідної їм для виконання своїх службових обов'язків. Такі фактори, як відповідальність, компетентність та повноваження, використовуються для визначення того, хто є достатньо відповідальним, щоб мати доступ до певної інформації. Це гарантує, що співробітники низького рівня не отримають доступ до конфіденційних даних бізнесу, які можуть бути використані проти компанії [9].

1.3 Огляд існуючих рішень

Міжмереві екрани

Міжмережевий екран (фаєрвол, брандмауер) являє собою апаратно-програмний комплекс засобів, які фільтрують локальний і вхідних трафік, згідно з параметрами, раніше заданих адміністратором. Головна мета використання міжмережевого екрану-захист інформації від зловмисників і фільтрація трафіку [1].

Міжмережевий екран - комплексний захист, який вважається обов'язковим для будь-якої корпоративної мережі. Крім фільтрації трафіку у міжмережевого екрану є ще одна важлива функція-захист конфіденційних даних від витоку, а також захист від несанкціонованого доступу до мережі шкідливого програмного забезпечення.

До допоміжних (другорядних) функцій фаєрвола екрану можуть відноситися:

- журналювання всіх подій;
- запис підозрілої активності;
- ведення обліку мережевого обладнання;
- аналіз використання портів і мережевих підключень;
- фільтрація різних типів даних тощо.

Брандмауер використовується для:

- Фільтрування трафіку, блокування додатків, які намагаються отримати доступ до незахищених системних служб.
- Запобігання несанкціонованому доступу до даних з боку зловмисників та припинення спроб відправки конфіденційної інформації.
- Забезпечення контролю доступу до мережевого обладнання та портів.
- Ведення логів в рамках мережі і запису активності додатків / обладнання в статистику.
- Надсилання повідомлень при виявленні підозрілої активності або спроб атакувати мережу підприємства.

Самостійно міжмережевий екран не здатний гарантувати повний захист мережевого обладнання від шкідливого програмного забезпечення та діяльності зловмисників. Міжмережевий екран не є альтернативою антивірусному ПЗ.

Найбільша ефективність роботи брандмауера може бути забезпечена при його роботі в комплексі з іншими захисними механізмами (обладнанням і ПЗ).

Вибираючи конкретний вид міжмережевого екрану, потрібно спиратися конкретно на вимоги системи підприємства.

Сканери вразливостей

Сканер вразливостей (Vulnerability scanner) - Програмне або апаратне комплексне рішення для сканування інформаційної інфраструктури в реальному часі. Сканер використовується для виявлення проломів в мережевому захисті, операційній системі, базах даних, додатках і т.д. головне завдання — оцінювати безпеку, виявляти уразливості і виводити звіти [6].

Адміністратор за допомогою сканера вразливостей може знаходити "дірки", якими користуються хакери для отримання несанкціонованого доступу до конфіденційних даних в мережі компанії. Також сканер

вразливостей може контролювати запущені процеси, служби і сканувати використовувані порти. Сканер вразливостей має наступний функціонал:

- шукає різні типи вразливостей мережі і аналізує їх в режимі реального часу;
- перевіряє ресурси мережі, операційні системи, підключені пристрої, порти;
- аналізує всі активні процеси, поведінку запущених додатків;
- створює звіти, в яких прописує тип уразливості

Принцип роботи сканера

Зондування. Найефективніший, але повільний метод активного аналізу. Суть його полягає в тому, що сканер сам проводить спроби експлуатації знайдених вразливостей і моніторить мережу, визначаючи, де можуть пройти загрози. У процесі зондування адміністратор може підтвердити здогадки щодо "дірок" і вжити заходів щодо їх закриття [4].

Сканування. У такому режимі сканер працює максимально швидко, але проводить аналіз лише на поверхневому рівні. Тобто "дивиться «на явні» дірки" і аналізує загальну безпеку інфраструктури. Відмінність цього механізму від попереднього в тому, що сканер вразливостей не підтверджує наявність уразливості, а лише попереджає про неї адміністратора [4].

Робота сканера базується на непрямих ознаках вразливостей. Наприклад, якщо сканер аналізує протоколи прикладного рівня або API, то він визначає їх параметри і порівнює з прийнятними значеннями, заданими адміністратором. Якщо він виявить розбіжність значень, адміністратор отримає повідомлення про потенційну уразливість. Після цього потрібно перевірити знайдені потенційні загрози будь-яким іншими інструментами.

Які дії виконує сканер вразливостей:

- Збирає інформацію з усієї інфраструктури: активні процеси, запущені додатки, працюючі порти і пристрої, служби і т. д.

– Шукає потенційні уразливості. Методом сканування (використовує непрямі ознаки уразливості без підтвердження її наявності) і зондування (запускає імітації атак).

– Використовує спеціальні методи моделювання атак, щоб підтвердити або спростувати присутність уразливості (функція доступна не в кожному сканері).

– Формує докладний звіт з інформацією про знайдені вразливості.

Сканери можуть бути «дружніми» або «агресивними». Перший тип просто збирає інформацію і не моделює атаку. Другий користується вразливістю, щоб викликати збій в роботі програмного забезпечення.

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) являє собою систему, яка збирає інформацію для подальшого аналізу та класифікації системним адміністратором або фахівцем з ІБ [1].

Спочатку SIEM складалося з двох напрямків: Security Information Management, яке відповідає за інформаційну безпеку, і Security Event Management, що контролює події безпеки. У 2005 році відбувається об'єднання понять, і з'являється Security Information and Event Management. Перед системою SIEM ставляться наступні завдання:

– Консолідація і зберігання журналів подій від різних джерел-мережевих пристроїв, додатків, журналів ОС, засобів захисту. Заглянувши в будь-який стандарт ІБ, ви побачите технічні вимоги по збору та аналізу подій. Вони потрібні не тільки для того, щоб виконати вимогу стандарту. Бувають ситуації, коли інцидент побачили пізно, а події вже давно затерті або журнали подій чомусь недоступні, і причини інциденту виявити фактично неможливо. Крім того, з'єднання з кожним джерелом і Перегляд подій займе багато часу. В іншому випадку, без аналізу подій, є ризик дізнатися про інцидент у вашій компанії з новинних стрічок.

- Надання інструментів для аналізу подій і розбору інцидентів. Формати подій у різних джерелах різняться. Текстовий формат при великих обсягах сильно стомлює, знижує ймовірність виявлення інциденту. Частина продуктів класу SIEM уніфікує події і робить їх більш читабельними, а інтерфейс візуалізує тільки важливі інформаційні події, акцентує на них увагу, дозволяє фільтрувати некритичні події.
- Кореляція та обробка за правилами. По одній події не завжди можна судити про інцидент. Найпростіший приклад « "login failed": один випадок нічого не означає, Але три і більше таких події з одним обліковим записом вже можуть свідчити про спроби підбору. У найпростішому випадку в SIEM правила представлені у форматі RBR (Rule Based Reasoning) І містять набір умов, тригери, лічильники, сценарій дій.
- Автоматичне оповіщення та інцидент-менеджмент. Основне завдання SIEM - не просто зібрати події, але автоматизувати процес виявлення інцидентів з документуванням у власному журналі або зовнішній системі HelpDesk, а також своєчасно інформувати про подію.

SIEM здатна виявляти:

- мережеві атаки у внутрішньому і зовнішньому периметрах;
- вірусні епідемії або окремі вірусні зараження, невдалені віруси, бекдори і трояни;
- спроби несанкціонованого доступу до конфіденційної інформації;
- фрод і шахрайство;
- помилки і збої в роботі інформаційних систем;
- уразливість;
- помилки конфігурацій в засобах захисту та інформаційних системах.

Система SIEM універсальна за рахунок своєї логіки. Але для того щоб покладені на неї завдання вирішувалися — необхідні корисні джерела і

правила кореляції. Будь-яка подія (наприклад, якщо в певній кімнаті відкрилися двері) може бути подано на вхід і використано.

Джерела вибираються на підставі наступних факторів:

- критичність системи (цінність, ризики) та інформації (оброблюваної і збереженої);
- достовірність та інформативність джерела подій;
- покриття каналів передачі інформації (повинні враховуватися не тільки зовнішній, але і внутрішній периметр мережі);
- вирішення спектру завдань ІТ та ІБ (забезпечення безперервності, розслідування інцидентів, дотримання політик, запобігання витоків інформації тощо).

Основні джерела SIEM:

- Access Control, Authentication - для моніторингу контролю доступу до інформаційних систем і використання привілеїв.
- Журнали подій серверів і робочих станцій — для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки.
- Мережеве активне обладнання (контроль змін і доступ, лічильники мережевого трафіку).
- IDS\IPS. Події про мережеві атаки, зміна конфігурацій і доступ до пристроїв.
- Антивірусний захист. Події про працездатність ПЗ, базах даних, зміні конфігурацій і політик, шкідливих програмах.
- Сканери вразливостей. Інвентаризація активів, сервісів, програмного забезпечення, вразливостей, поставка інвентаризаційних даних і топологічної структури.
- GRC-системи для обліку ризиків, критичності загрози, пріоритизації інциденту.

- Інші системи захисту і контролю політик ІБ: DLP, антифрода, контролю пристроїв і т. п.
- Системи інвентаризації та asset-management. З метою контролю активів в інфраструктурі та виявлення нових.
- Netflow і системи обліку трафіку.

Рішення SIEM включає в себе, як правило, кілька компонентів:

- агенти, що встановлюються на інспектовану інформаційну систему (актуально для операційних систем; агент являє собою резидентну програму (сервіс, демон), яка локально збирає журнали подій і по можливості передає їх на сервер);
- колектори на агентах, які, по суті, являють собою модулі (бібліотеки) для розуміння конкретного журналу подій або системи;
- сервери-колектори, призначені для попередньої акумуляції подій від безлічі джерел;
- сервер-корелятор, що відповідає за збір інформації від колекторів і агентів і обробку за правилами і алгоритмами кореляції;
- сервер баз даних і сховища, що відповідає за зберігання журналів подій.

Дані про події збираються від джерел за допомогою встановлених на них агентів, або віддалено (за допомогою з'єднання по протоколах NetBIOS, RPC, TFTP, FTP). У другому випадку неминуче виникає навантаження на мережу і джерело подій, так як частина систем не дозволяє передати тільки ті події, які ще не були передані, і передає в сторону SIEM весь журнал подій, що становить часто сотні мегабайт. Затирати ж журнал подій на джерелі при кожному зборі даних-некоректно [1].

Події повинні не тільки збиратися в консолідоване сховище для розбору за фактом інциденту, а й оброблятися. В іншому випадку ви отримаєте рішення, яке повністю не виправдовує витрати. Безумовно, інструментарій SIEM скоротить час, необхідний для розбору інциденту.

Але завдання SIEM-своєчасно виявляти, запобігати загрозам і оперативно реагувати на них. Для цього необхідно складати правила кореляції - з урахуванням актуальних для компанії ризиків. Ці правила не перманентні і повинні постійно актуалізуватися експертами. Як і у випадку з правилами для систем виявлення вторгнень, якщо вчасно не прописати правило, що дозволяє виявляти типову загрозу, - вона буде, швидше за все, реалізована. Переваги SIEM перед IDS в правилах-можливість вказувати загальний опис симптомів і використання накопиченої статистики baseline для спостереження за відхиленнями від нормальної поведінки інформаційних систем і трафіку.

1.4 Висновки першого розділу

В цьому розділі було розглянуто поняття несанкціонованого доступу, важливість цієї проблеми та можливі наслідки. Після цього було зосередженно увагу на питанні попередження несанкціонованого доступу до інформуції – одному з чотирьох етапів протидії цьому явищу та засоби боротьби з НСД саме на цьому етапі. Найсучасніші та найефективніші щасоби було детально вивчено та наведенно методи їх роботи і основні переваги. Також було дослідженно питання процесу авторизації та методів її реалізації, як одного з засобів попередження НСД.

Робота, проведенна в цьому розділі, розширила обізнанність, щодо такої загрози як НСД та методів протидії цій загрозі на етапі попередження, ці знання будуть дуже корисними при виконнані кваліфікаційної роботи бакалавра та в подальшій професійний діяльності.

2 ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ДЛЯ ПОБУДОВИ СИСТЕМИ

2.1 Управління доступом на основі ролей

Як вже було зазначено у першому розділі, управління доступом на основі ролей (role-based access control або RBAC) - це метод обмеження доступу до мережі на основі ролей окремих користувачів в рамках підприємства. RBAC дозволяє співробітникам мати права доступу тільки до тієї інформації, яка їм необхідна для роботи, і не дозволяє їм отримувати доступ до інформації, яка у них не відноситься [9].

Роль співробітника в організації визначає дозволи, які йому надаються, і гарантує, що співробітники нижчого рівня не зможуть отримати доступ до конфіденційної інформації або виконати завдання високого рівня. У моделі даних, що використовує контроль доступу на основі ролей, ролі засновані на декількох факторах, включаючи авторизацію, відповідальність і професійну компетентність. Таким чином, компанії можуть вказати, чи є людина кінцевим користувачем, адміністратором або спеціалізованим Користувачем. Крім того, доступ до ресурсів може бути обмежений конкретними завданнями, такими як можливість перегляду, створення або зміни файлів.

Обмеження доступу до мережі є важливим для організацій, у яких багато працівників, а також для тих, хто наймає підрядників або дозволяє доступ до ресурсів третім особам, таким як Клієнти та постачальники, що ускладнює ефективний моніторинг доступу до мережі. Компанії, які застосовують RBAC, можуть краще захистити свої конфіденційні дані та критично важливі програми.

Використання RBAC для обмеження непотрібного доступу до мережі на основі ролей користувачів в організації має ряд переваг, в тому числі:

- Підвищення операційної ефективності. Завдяки RBAC компанії можуть знизити потребу в зміні документів і паролів, коли наймають нових співробітників або змінюють ролі існуючих співробітників. RBAC дозволяє організаціям швидко додавати і змінювати ролі, а також реалізовувати їх на різних платформах, в операційних системах і додатках. Це також скорочує ймовірність помилки при призначенні прав користувача. Крім того, за допомогою RBAC компанії можуть легше інтегрувати сторонніх користувачів у свої мережі, надаючи їм зумовлені ролі.
- Підвищення відповідності. Кожна організація повинна відповідати місцевим, державним і федеральним нормам. Компанії зазвичай вважають за краще впроваджувати системи RBAC для задоволення нормативних і законодавчих вимог щодо конфіденційності, оскільки керівники та IT-відділи можуть більш ефективно управляти доступом і використанням даних. Це особливо важливо для фінансових установ та медичних організацій.
- Прозорість і контроль. RBAC надає системним адміністраторам більше прозорості та контролю, а також гарантує, що авторизованим користувачам і гостям в системі надається доступ тільки до того, що їм потрібно для виконання своєї роботи.
- Скорочення витрат. Заборонивши користувачеві доступ до певних процесів і додатків, компанії можуть економити або більш ефективно використовувати ресурси, такі як пропускна здатність мережі, пам'ять і сховище.
- Зниження ризику порушень і витоку даних. Впровадження RBAC означає Обмеження доступу до конфіденційної інформації, що знижує ймовірність злому або витоку даних.

Для виконання завдання був обраний саме цей метод контролю доступу, адже він ідеально підходить для впровадження авторизації в корпоративній мережі.

2.2 Мова програмування PHP

PHP-це мова програмування, яка використовується для створення сучасних динамічних сторінок на сайтах. У перекладі з англійської абревіатура PHP перекладається як «попередній обробник гіпертексту». PHP є мовою опису скриптів, яку можна впроваджувати в HTML. В основі її синтаксису лежить C, Perl і Java, з додаванням декількох особливостей, специфічних саме для PHP. Мета створення PHP є надання можливостей створювати динамічно генеровані сторінки.

Код, написаний на PHP, спрямований на виконання двох завдань:

- html-частина відповідає за зовнішній вигляд і відображення інформації;
- php-частина, інтегрована в html, забезпечує можливості інтерактивності і динаміку.

При цьому подібні програмні коди і, відповідно, складені з їх допомогою проекти, є легкими, ефективними, гнучкими, багатофункціональними, зручними в адмініструванні, редагуванні, обслуговуванні.

На сьогоднішній день переважна більшість сайтів, сервісів і додатків, а також такі популярні платформи як Joomla, Drupal, WordPress, 1C-Bitrix і UMI.CMS написані саме на PHP-мові.

Мова PHP має ряд незаперечних переваг:

- Висока швидкість роботи і, відповідно, загальна продуктивність ресурсів.
- Бюджетність, економічність. Знайти фахівця не представляється проблемою, вартість написання програм на php не висока.
- Простота освоєння, простий синтаксис.
- Відмінна сумісність і переносимість — PHP-коди працюють однаково добре з різними платформами.

- Набір тексту коду і його редагування можна здійснювати в будь-якому текстовому або html-редакторі.
- Висока гнучкість, ємність і функціональність. PHP-програму можна складати окремо від розробки веб-сторінки, без прив'язки, після чого поєднати. Це істотно спрощує життя дизайнерів і програмістів.
- Багатозадачність і широкі можливості — створення будь-яких веб-додатків, блогів, гостьових книг, інтернет-магазинів, сайтів, робота з редиректами, заголовками, pdf-документами, базами даних, електронною поштою та ін.

Для розробки програмного забезпечення була обрана мова програмування PHP, адже вона добре підходить для розробки цільового функціоналу завдяки перевагам вказаним вище до яких слід додати можливість розробки з допомогою об’єктно орієнтованого підходу до програмування, саме ця можливість дозволить розробити ПЗ, функціонал якого мого можна з легкістю розширити за необхідності.

2.3 Висновки

В даному розділі було більш детально розглянуто модель контролю доступу на основі ролей та її переваги, дана модель була вибрана, адже вона дозволяє з легкістю надавати доступ до необхідного функціоналу новим та тимчасовим працівникам та значно полегшує роботу працівників безпеки, тобто, вагомо знижує ризик внутрішніх порушень та витоків кінфіденційної інформації.

Також було наведенно деякі твердження, щодо мови програмування PHP, яка використовуватиметься в розробці, що обґрунтовано її первагами, які є дуже важливими в даному випадку.

3 АНАЛІЗ БЕЗПЕКИ РЕКЛАМНОГО АГЕНСТВА

3.1 Аналіз діяльності підприємства

Рекламне агентство отримує рекламне замовлення від фізичної або юридичної особи, здійснює контроль виробництва реклами і контролює поширення на рекламних носіях або комунікаційних каналах, по яких рекламний продукт досягає кінцевого користувача. Крім того здійснює завдання з аналізу, планування та оцінки ефективності рекламної кампанії, також надає і різні рекламні послуги. У комплексі рекламні послуги включають в себе великий список різноманітних завдань, що представляють собою поєднання інтелектуальної та фізичної праці. До нематеріальної частини послуг можна віднести всю сервісну і творчу частину рекламного процесу; до матеріальної частини — всю виробничу область (рекламне виробництво). Різноманітність видів діяльності рекламного агентства відображає широкий спектр завдань, яке воно може виконувати.

Структурна схема підприємства зображена на рисунку 3.1.

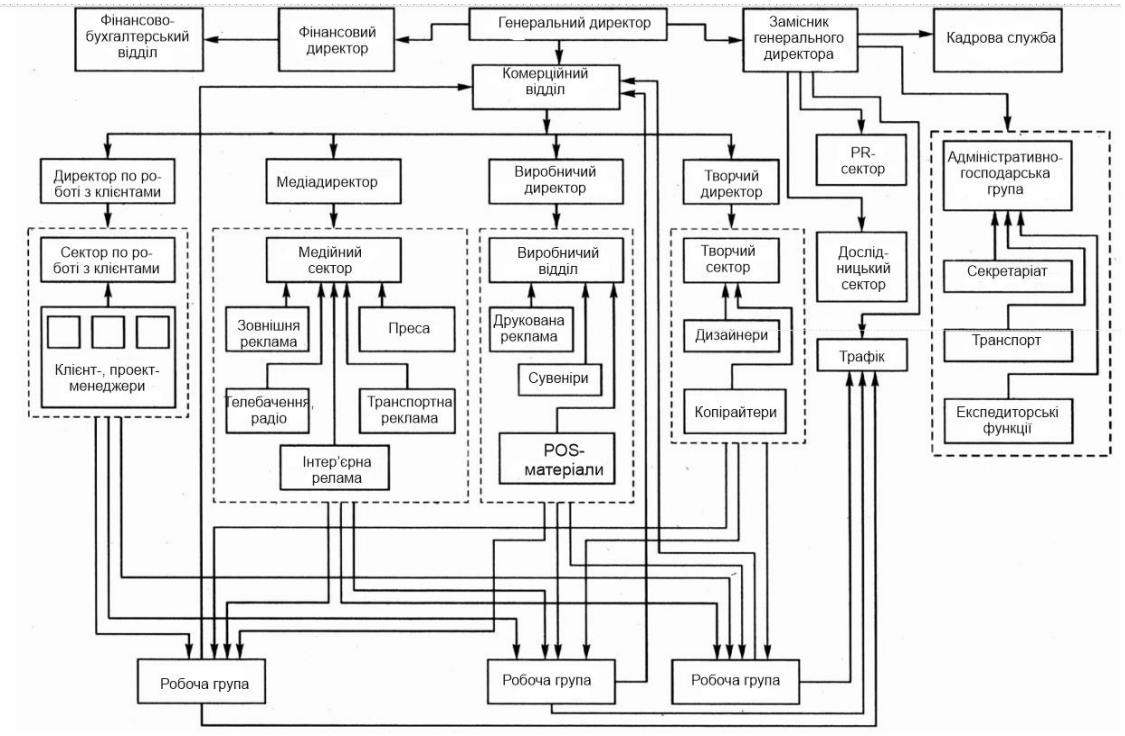


Рисунок 3.1 – Структурна схема підприємства

1. Відділ по роботі з клієнтами

Відділ по роботі з клієнтами структурно ділиться на робочі групи, кожна з яких веде справи окремого Клієнта. До складу робочих груп для виконання конкретного замовлення клієнтів входять представники творчого, виробничого відділів та відділу маркетингу. Після постановки цілей робоча група готує пропозицію по бюджету для узгодження з клієнтом. Потім його співробітники, в контакті з іншими відділами, розробляють концепцію рекламного звернення, план рекламної кампанії і так далі. Концепція повинна утвердитися клієнтом і представниками керівництва агентства, а іноді експертною радою агентства. Після цього починається процес кінцевого доопрацювання рекламного плану і уточнення всіх деталей. Керівник групи представляє інтереси агентства на переговорах з клієнтом та інтереси клієнта всередині свого агентства, представляє клієнту підготовлені агентством пропозиції, поради та напрацювання. Він контролює всю роботу по виконанню замовлення від

початку до кінця і підпорядкований директору по роботі з клієнтами. Директор по роботі з клієнтами звітує перед радою директорів агентства, відповідає за прибутковість проектів, веде переговори з новими клієнтами. У великих агентствах при наявності великої кількості клієнтів з'являється тимчасова Посада трафік-менеджера, який постійно відстежує хід роботи замовлень клієнтів, контролює діяльність підконтрольних ділянок, залучених в розробку і виконання рекламних кампаній. Відділ по роботі з клієнтами є «візитною карткою» агентства: саме він визначають характер взаємин агентства з клієнтом і на основі результатів його діяльності у клієнта формується думка про роботу агентства в цілому.

2. Творчий відділ

Творчий відділ спеціалізується на роботі в області формування рекламного продукту — формуванню вихідних творчих завдань, креативних рекламних концепцій, самих творчих рішень реклами і створення власне рекламних кампаній для клієнта-рекламодавця. Завдання співробітників творчого відділу вкрай висока, так як від їх навичок і таланту залежить ефективність впливу створюваної реклами. Саме вони виконують генерування ідей рекламного звернення і знаходять кінцеві варіанти засобів їх здійснення. Творчий відділ об'єднує художніх редакторів, художників-дизайнерів, фахівців-графіків, текстовиків. Іноді до складу відділу включаються і інші творчі фахівці. Відділ підпорядковується директору творчої служби. У великих агентствах робота творчого відділу координується редакційно-художньою радою.

3. Виробничий відділ

Виробничий відділ спеціалізується на роботах з виготовлення розробленої агентством реклами. З цією метою відділ підтримує відносини з підрядниками — спеціальними фірмами, що володіють виробничими потужностями (виробниками і постачальниками різних елементів рекламного витратного матеріалу, друкарнями, іншими допоміжними

організаціями, діяльність яких пов'язана із створенням рекламного продукту), у яких розміщує замовлення на рекламні продукти і контролює їх виконання (це можуть бути, наприклад, блогери, поліграфічна продукція, сувенірна продукція, відеоролики для інтернету та ТБ, аудіозаписи для радіо і багато іншого).

4. Медійний відділ

Медійний відділ займається плануванням і розміщенням розробленої агентством реклами в засобах поширення реклами — здійснює вибір каналів поширення реклами (медіапланування), виконує дослідження в засобах масової інформації та інших видах рекламних носіїв, займається закупівлею рекламного простору (медіабаїнг) відповідно до складеного плану рекламної кампанії. Ще в завдання відділу входить контроль над підготовкою та виконанням рекламних кампаній, моніторинг актуальних висновків реалізації рекламних звернень. Відділ виконує аналіз для клієнтів агентства, виконує повний обсяг роботи з підрядниками (власниками рекламних мереж, представниками засобів масової інформації або їх агентствами). Відділ об'єднує фахівців з медіапланування, медіабаїнгу та медіамоніторингу. Характеристики виконаної роботи відділу визначаються якістю підготовлених медійних планів і програм, і так само контролем над їх виконанням.

5. Адміністративний відділ

Адміністративний відділ здійснює управління будь-якою діяльністю рекламного агентства. Відділ містить фахівців бухгалтерського обліку, фахівців з аналітики, розробки та контролю над реалізацією поставлених фінансових планів, регулювання доходів і витрат, встановлення поточної політики, а також безпосередньо адміністраторів — від президента або директора до керівників інших відділів. У великих агентствах адміністративний відділ може також включати додаткові допоміжні

підрозділи, такі як відділ кадрів, господарський відділ, технічна служба, кур'єрська служба та інші, або створюються тимчасові необхідні групи.

6. Виробничий відділ

Виробничий відділ займається виготовленням рекламних носіїв і в окремих випадках об'єднує друкарню, майстерні з виробництва рекламних банерів та інші необхідні виробничі підрозділи.

Тут фахівці розробляють рекламний макета-малюнок, на якому зображуються всі елементи майбутньої реклами.

7. Відділ маркетингу

У відділі маркетингу рекламного агентства працюють фахівці з розповсюдження реклами, проведення маркетингових досліджень і заходів щодо стимулювання збуту. Найчастіше відділ маркетингу займається плануванням, закупівлями, проводить дослідження, визначає місце компанії на ринку, пошуком більш вигідних позицій в конкурентному середовищі.

Співробітники відділу маркетингу стежать за зміною аудиторії засобів реклами, розробляють плани по використанню кожного рекламного носія в кожній конкретній ситуації, закуповують рекламні місця. Фахівці відділу маркетингу готують докладні поради щодо необхідності і вимог споживачів, їх ставлення до бренду клієнта і того, як реклама могла б ефективно допомагати запитам споживачів.

8. Фінансово-господарський відділ

Крім безпосереднього виконання своїх завдань, рекламне агентство повинно правильно і вміло вести свою фінансово-господарську діяльність і забезпечувати нормальне управління виробничим процесом. Для цього і існує така допоміжна служба, як фінансово-господарський відділ, який може включати в себе бібліотеку, відділ кадрів та інші необхідні структурні підрозділи.

Фінансовий відділ повинен своєчасно виставляти клієнтам рахунки на оплату послуг, регулювати виробничі витрати, контролювати правильне

відображення витрат у відповідних фінансових документах, вести нарахування заробітної плати, сплачувати податки і виконувати інші фінансові завдання.

3.2 Інформаційні ресурси та потоки підприємства

В таблиці 3.1 описані всі інформаційні ресурси підприємства, їх рівні секретності і доступу.

Таблиця 3.1 - Інформаційні ресурси підприємства.

Інформаційний ресурс	*Тип інформації*	*Рівень конфіденційності*	*Підрозділи, працівники яких допущенні до інформації*	*Де зберігається і обробляється інформація*	*Носії, які використовуються для зберігання інформації*
Виробнича інформація	Загальнодоступна	Базовий	Всі	Серверна, кімната охорони	Електронні та паперові
Управлінська інформація	Обмежений доступ	Середній	Директори, бухгалтерія, адміністративний відділ	Серверна, кімната охорони	Електронні та паперові
Інформація пов’язана з безпекою і персональними даними	Обмежений доступ	Підвищений	Директори, бухгалтерія	Серверна, кімната охорони	Електронні

Таблиця 3.2 - рівні конфіденційності інформації на підприємстві

Рівень конфіденційності інформації	*Опис*
Базовий	Мінімальна секретність. Зазвичай, призначається внутрішнім відкритим документам
Середній	Призначається службовим матеріалам
Підвищений	Підвищена секретність. Призначається матеріалам, що містять персональні дані, інформацію про фінансову діяльність та ін.

На рисунку 3.2 можна розглянути інформаційні потоки підприємства

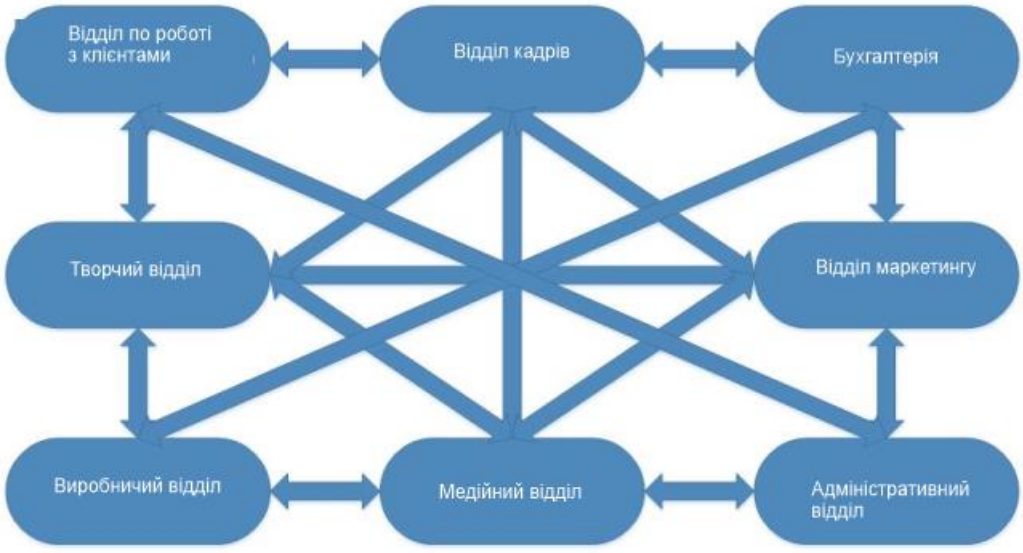


Рисунок 3.2 – Інформаційні потоки підприємства

1. Горизонтальні інформаційні потоки

Часто вони приймають неофіційний характер але бувають і винятки. Найефективнішими інформаційними потоками є горизонтальні, з точки зору комунікації в колективі. Тут залишається близько 90%

переданих даних. Це означає, що втрата інформації за передачі таким чином мінімальна щодо інших. Пояснити це можна тим, що людям, які знаходяться на одному щаблі службової ієрархії, психологічно легше зрозуміти колегу, адже вони вирішують схожі завдання, стикаються з подібними проблемами, працюють в одному відділі або часто контактують сусідніми відділами.

2. Низхідні інформаційні потоки

Вони мають формальний і неформальний характер. З боку їх комунікативної ефективності, справа проходить наступним чином: з кожним наступним проміжною ланкою проходить спадна інформація більше вона втрачається і змінюється. Відбувається незворотний процес спотворення отриманих даних. На практиці кожен вищестоящий керівник повинен розуміти, що кожна передавальна Ланка може «втрачати» до 50% прийнятої інформації.

Парадокс полягає в тому, що одержана від начальства інформація не приховується і не спотворюється кимось свідомо або спеціально; проблема полягає в повноті передачі, так звані "комунікативні бар"єри". При низхідних інформаційних потоках простежується ефект "зіпсованого телефону".

3. Висхідні інформаційні потоки

Вони дуже рідко бувають неформальними, це не має необхідності в поясненні. Спотворення інформації здатне досягти 90%! Найцікавіше, що інформація, яка тут міститься, найменше перевіряється. Якщо на підприємстві, у фірмі або установі не встановлено приплив ідей знизу, ймовірно, можливості для його інноваційного розвитку досить обмежені.

3.3 Модель загроз інформаційній безпеці

Під аналізом вразливостей розуміються процеси, спрямовані на пошук будь-яких загроз, вразливих точок і ризиків потенційного несанкціонованого проникнення зловмисників в ІС (інформаційну систему).

Вразливість-слабкий компонент ІС будь-якої організації. Загроза-можливість негативного впливу з боку зловмисників, яке може спричинити компрометацію комерційної та іншої конфіденційної інформації. Третя особа в такому аналізі-зловмисник, який використовує уразливості для реалізації загроз [8]

Якщо присутні уразливості, це негативно позначається на роботі всього підприємства, так як воно стає менш захищеним перед недобросовісними конкурентами, це спрощує роботу зловмисників з нанесення шкоди і дозволяє третім особам отримати доступ до конфіденційних даних.

Ефективна ІБ забезпечує не тільки захист від крадіжки будь-яких даних з мережі підприємства, але і фінансовий захист бізнесу в цілому. Підприємства, які хочуть відрізнятися якісною ІБ, постійно працюють над запобіганням:

- витоків будь-яких корпоративних даних
- віддаленого редагування захищеної інформації
- зміни рівня захисту від загроз, які можуть спровокувати втрату довіри інвесторів, постачальників, контрагентів тощо.

Загрози можуть мати кілька джерел, тому дуже важливо своєчасно їх класифікувати і створити схему їх аналізу. Це дозволить отримати найбільше охоплення потенційних вразливостей в бізнес-процесах підприємства.

В ІБ вкрай важливо слідувати чотирьом принципам:

- конфіденційність

- цілісність
- достовірність
- доступність

Джерело загрози може бути як випадковим, так і навмисним. Третій варіант-техногенні та природні фактори, які ніколи не варто виключати.

У кожної загрози є свій список вразливостей, за допомогою яких зловмисник може реалізувати свої плани. Щоб провести якісний аналіз вразливостей інформаційної структури, необхідно розрізняти види загроз, які можуть виникнути в системі конкретної організації. Такі загрози поділяються на окремі класи [5].

1 клас. Потенційне джерело загрози, яке може перебувати:

- безпосередньо в інформаційній системі (ІВ)
- в межах видимості ІС (наприклад, пристрої для несанкціонованого звукозапису)
- поза зоною видимості ІС (перехоплення даних в процесі їх відправки куди-небудь)

2 клас. Вплив на ІС, який може нести:

- активну загрозу (троян, вірус)
- пасивну загрозу (копіювання конфіденційної інформації зловмисником)

3 клас. Метод забезпечення доступу, який може бути реалізований:

- безпосередньо (крадіжка паролів)
- за допомогою нестандартних каналів зв'язку (наприклад, уразливості операційної системи)

Головні цілі атаки на ІТ-інфраструктуру компанії:

- отримання контролю над цінними ресурсами і даними
- організація несанкціонованого доступу до корпоративної мережі

- обмеження діяльності підприємства в певній галузі

Другий метод найчастіше реалізується на замовлення недобросовісних компаній-конкурентів або політичними діячами.

Що конкретно може нести загрозу інформаційній безпеці будь-якого підприємства:

- шкідливе програмне забезпечення
- шахраї-хакери
- інсайдери-працівники, які діють зі злими намірами або з необережності
- природні явища

Реалізувати загрозу можна декількома методами. Наприклад, організувати перехоплення даних, залишити програмну або апаратну «закладку» або порушити роботу локальних бездротових корпоративних мереж, організувати для інсайдерів доступ до інфраструктури компанії [5].

Оцінка ймовірності загроз

Для оцінки ймовірності настання загрози професіоналами застосовується якісна шкала, що складається з трьох рівнів. Розглянемо їх докладніше.

Рівень 1-Н ("низька ймовірність»)

Відрізняється мінімальною ймовірністю появи. У такої загрози немає ніяких передумов (минулих інцидентів, мотивів) для того, щоб вона була реалізована. Загрози рівня Н, як правило, виникають не частіше, ніж 1 раз в 5 – 10 років [8].

Рівень 2-С ("середня ймовірність»)

У такої загрози ймовірність виникнення трохи вище, ніж у попередньої, тому, що в минулому, наприклад, вже були подібні інциденти або відомо, що атакуюча сторона має плани по реалізації такої загрози. Загрози з рівнем с призводять до інцидентів приблизно раз на рік [8].

Рівень 3-В ("висока ймовірність»)

Загроза має високі шанси на реалізацію. На підтвердження тому- статистична інформація, наявність подібних інцидентів у минулому, серйозна мотивація з боку зловмисників. Ймовірна частота виникнення загроз рівня в-раз на тиждень або частіше.

Методики аналізу вразливостей

Існує кілька способів, за допомогою яких можна провести аналіз вразливостей системи. Один з них заснований на імовірнісної методикою, і при його застосуванні потрібно спиратися на наступні фактори:

- потенціал зловмисника (виявляється шляхом оцінок експертів)
- джерело загрози (де можлива атака - в зоні видимості або за її межами)
- метод впливу (мережевий, апаратний або соціальний)
- об'єкт загрози (корпоративні дані, засоби для шифрування, передачі, роботи з ними або співробітники компанії)

У процесі аналізу вразливостей в інформаційній системі вкрай важливо враховувати можливі місця дислокації. Щоб це реалізувати, потрібно оперативно виявити і усунути помилки в операційній системі і програмному забезпеченні, а пізніше систематично встановлювати всі патчі безпеки від розробників.

Аналіз вразливостей, які пов'язані з неправильним налаштуванням захисних засобів, повинен проводитися регулярно. Ідеальне рішення- налаштувати безперервний моніторинг ІВ на предмет виникнення вразливостей. Окремо від вищеописаного аналізу в обов'язковому порядку необхідно проводити певні заходи з робочим персоналом компанії: видавати права доступу до даних і ресурсів, права на установку спеціалізованого програмного забезпечення, а також права на копіювання інформації і застосування зовнішніх носіїв даних [2].

Після проведення аналізу загроз було сформовано схему (Рисунок 3.3), на якій вказані ймовірні загрози.

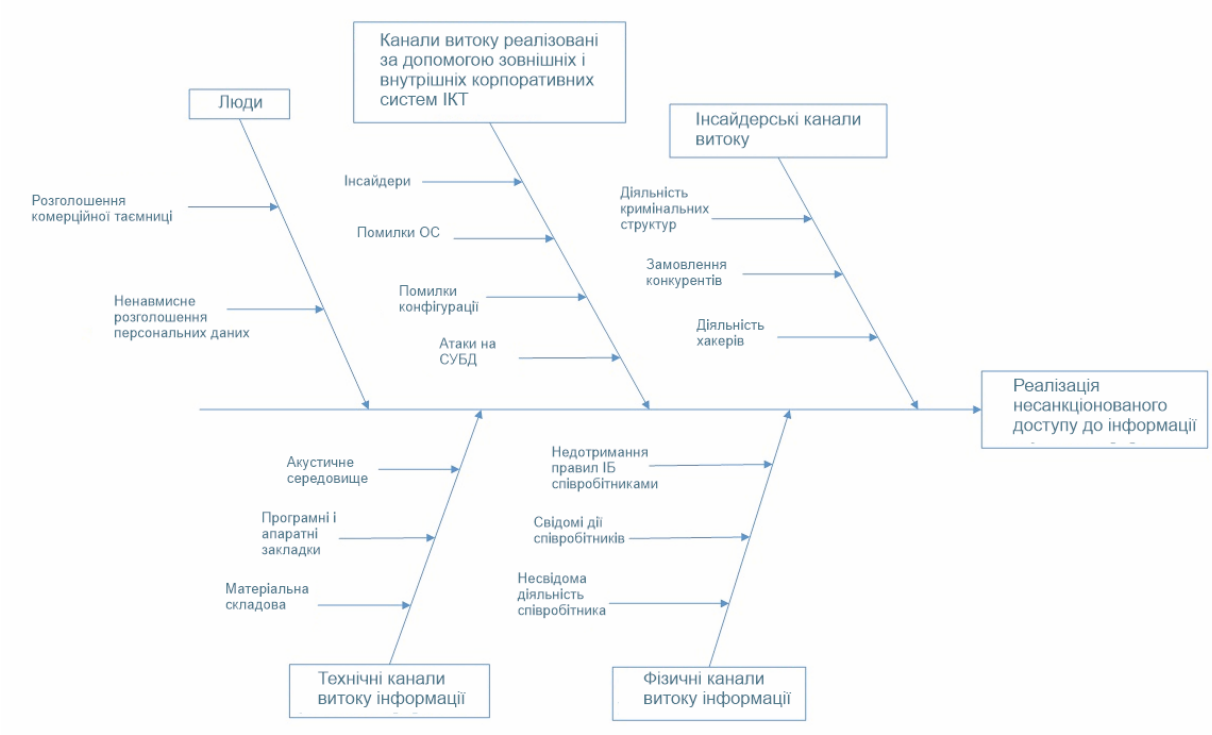


Рисунок 3.3 – Загрози інформаційній безпеці підприємства

3.4 Висновки

В третьому розділі було досліджено специфіку діяльності рекламного агенства, його структуру та основні завдання підрозділу. Було розподілено інформаційні ресурси на рівні секретності та проаналізовано можливі загрози інформаційній діяльності підприжмства.

4 РОЗРОБКА СИСТЕМИ АВТОРИЗАЦІЇ

4.1 Типова система авторизації з контролем доступу

На рисунку 4.1 зображена типова схема авторизації.

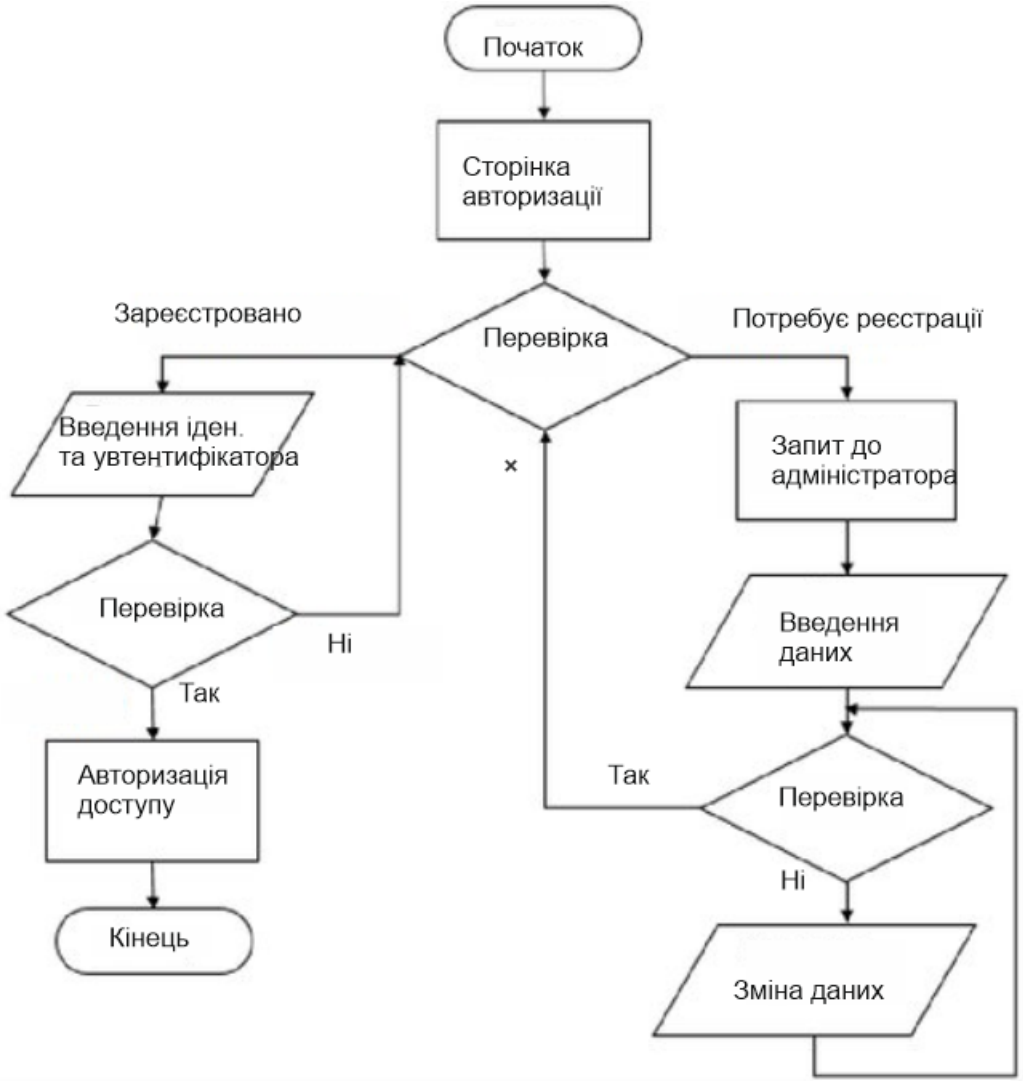


Рисунок 4.1 – Типова схема авторизації

Авторизація доступу важливий процес проте для надійності йому повинні передувати процеси індентифікації та автентифікації під час яких користувач надає надає свій особистий ідентифікатор(логін, номер телефону, адреса електронної поштової скриньки, або порядковий номер) та

підверджує свою особу за допомогою автентифікації(введення паролю, одноразового ключа, або за допомогою делегованої автенфікації, тобто, підвердження особистості через довірений сервіс на якому користувача вже авторизовано). Оскільки, основною метою авторизації є контроль та розмежування досутупу(в даному випадку на основі ролей(рисунок 4.2)), після проходження процесу авторизації користувачу надається доступ до певних дій, передбачених набором його ролей.

Рисунок 4.2 – схема розмежування доступу на основі ролей

Гранульоване управління доступом на основі ролей (RBAC) дозволяє управляти діями, які користувач може виконувати в межах інформаційної системи. Крім іншого, ролі контролюють доступ до функцій, даних і навіть документів [10].

Існує ряд передових методів, яким повинні слідувати організації при впровадженні BSC, в тому числі:

- Необхідно визначити ресурси, доступом до яких потрібно управляти, якщо вони ще не перераховані, наприклад, бази даних клієнтів, системи електронної пошти і т. д.

- Потрібно провести аналіз робочої сили і визначення ролей з однаковими потребами в доступі. Однак не варто створювати занадто багато ролей, оскільки це суперечить цілям RBAC і створює систему контролю доступу на основі конкретного користувача, а зовсім не його ролі. Наприклад, може існувати Базова роль користувача, яка включає доступ, необхідний кожному співробітнику, наприклад, до електронної пошти та корпоративної інтрамережі. Інша роль може бути роллю представника служби підтримки клієнтів, яка матиме права на читання / запис в базі даних клієнтів, і ще однією роллю може бути роль адміністратора бази даних клієнтів з повним контролем над нею[9, 10] .

- Після створення списку ролей і їх прав доступу потрібно налаштувати ці права і видати їх користувачам мережі.

- Потрібно визначити процес зміни ролі, блокування облікового запису співробітника, який залишає компанію, і процес реєстрації нових співробітників.

- Потрібно переконатися, що RBAC інтегрований у всі системи компанії.

- Також необхідно проводити навчання, щоб співробітники розуміли принципи RBAC.

- Періодично треба проводити аудит ролей, коректності їх призначення співробітникам і параметрів доступу, дозволеного для кожної ролі. Якщо з'ясовується, що роль має непотрібний доступ до певної системи, змініть роль і змініть рівень доступу для тих осіб, які знаходяться на цій ролі.

4.2 Розробка бази даних

Розробка бази даних важливий проектування будь-яких систем, система авторизації не є вийнятком. Адже помилки в проектуванні бази даних можуть спричинити несправності роботи програмного забезпечення, а це вже ризик утворення загрози.

Для створення бази даних була використана мова структурованих запитів SQL.

Діаграма таблиць зображена рисунку 4.3

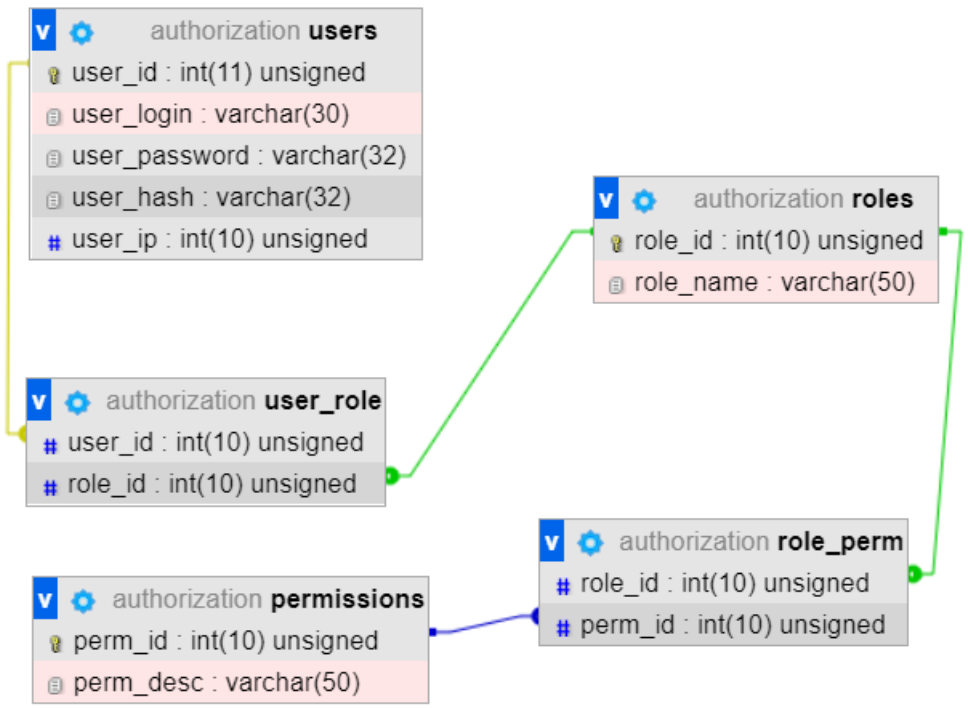


Рисунок 4.3 – Діграма таблиць бази даних

Першою розглянемо таблицю users, в ній будуть розміщуватись дані користувачів при реєстрації.

Поле user_id призначене для зберігання унікального ідентифікатора користувача(ціле число, яке інкрементується на одиницю для кожного нового користувача)

Поля user_login та user_password призначенні для зберігання логіну та паролю користувача відповідно, логіном може слугувати номер телефону або адреса поштової скриньки, пароль – це набір символів, який використовуватиметься для автентифікації після введення логіну. Пароль поміщається в таблицю після подвійного md5 шифрування.

User_hash – таблиця в яку після авторизації записуватиметься хешований рядок, який містить логін та пароль(в тому випадку, коли вони співпали).

User_ip – таблиця для зберігання ip-адреси користувача.

Наступні 4 таблиці призначенні для зберігання інформації про ролі та привілегії, які ними надаються. В таблиці roles зберігатимуться ідентифікатори та назви ролей, в таблиці permissions міститимуться ідентифікатори та описи привілегій(дій, дозволених носієві ролі в межах системи) , таблиця role_perm створена для відповідностей ролей та привілегій, а таблиця user_role для відповідностей користувачів та їхніх ролей.

Переважна більшість даних з бази даних не дуже цінна, адже знання про ролі та повноваження, які ними надаються не надасть достаньо інформації для атаки. Найважливішим є пароль користувача, для його захисту використовується влаштована в стандарний функціонал PHP функція шифрування MD5, пароль шифрується цією функцією 2 рази, за достатньої надійності паролю розшифрування може зайняти місяці або ж навіть роки.

4.3 Розробка системи авторизації та розмежування доступу

4.3.1 Розробка класів розмежування доступу

В першу чергу було рощроблено клас Role. Головна мета цього класу – повернути об’єкт ролі, в якому міститиметься список повноваженнь, які відповідають цій ролі та перевірка повноважень, для цього використовуються методи getRolePerms та hasPerm.

Однак, цього функціоналу замало, адже в організаціях з великою кількість співробітників процес створення нових ролей, призначення чи відбирання ролей в зв’язку з потоком кадрів є постійним протягом часу існування самої системи, тому необхідно додати функціонал, який дозволить додавати нові та видаляти застарілі ролі, надавати та відбирати ролі працівникам без особливих зусиль. В зв’язку з цим, клас Role було доповнено відповідними методами insertRole, insertUserRoles deleteRoles.

Прикладом слугуватиме програмна реалізація методу insertRole:

```
// Додати в таблицю нову роль
public static function insertRole($role_name) {
    $sql = "INSERT INTO roles (role_name) VALUES (:role_name)";
    $sth = $GLOBALS["DB"]->prepare($sql);
    return $sth->execute(array(":role_name" => $role_name));
}
```

Далі додамо клас клас PrivilegedUser, який дозволить наповняти ролі повноваженнями, перевіряти користувача на наявність певних повноважень та ролей, редагувати ролі, додаючи чи видаляючи окремі повноваження. Цейфункціонал реалізовують методи getByUsername, initRoles, hasPrivilege, insertPerms, deletePerms.

В якості прикладу наведено метод deletePerms:

```
// видалення повноважень з ролі
public static function deletePerms() {
    $sql = "TRUNCATE role_perm";
    $sth = $GLOBALS["DB"]->prepare($sql);
    return $sth->execute();
}
```

4.3.2 Розробка скриптів реєстрації та авторизації

В першу чергу слід розробити скрипт для реєстрації нового користувача. Користувач вводить в форму необхідні дані, скрипт перевіряє їх відповідність встановленим правилам та в разі успіху додає користувача в таблицю users.

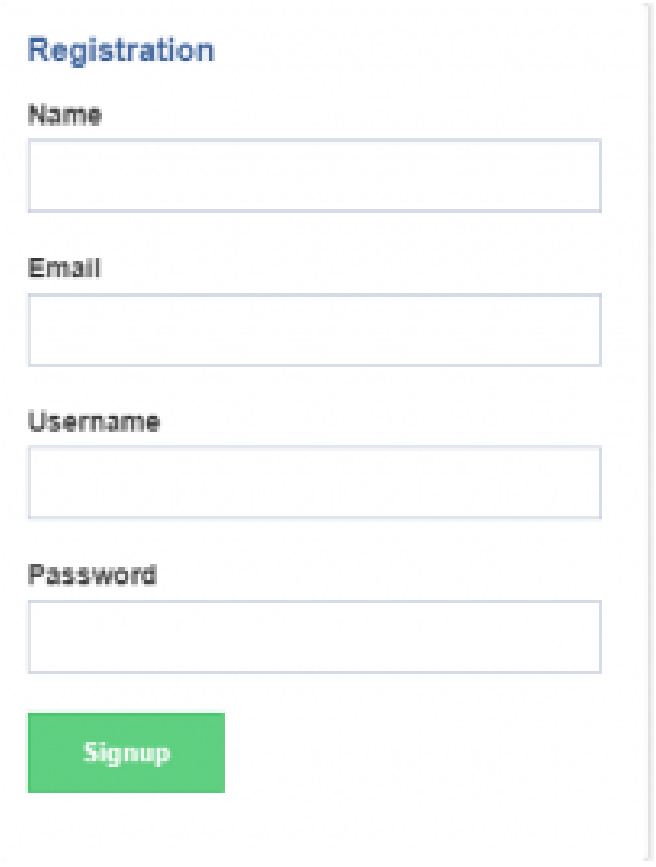


Рисунок 4.4 – Форма реєстрації

Спершу здійснюється підключення до бази даних,далі скрипт продовжить роботу після натискання кнопкм підтвердження, в ході виконання скрипта виконується перевірка введенних користувачем даних на відповідність вимогам, потім здійснюється запит для пошуку логіну користувача в базі даних з метою уникнення створення двох однакових облікових записів. В разі відсутності помилок пароль шифрується і дані додаються в базу даних, в протилежному випадку виводиться повідомлення про помилку.

Для функціонування авторизації потрібен ще один скрипт check.php, він потрібен для порівняння хешованого рядка в базі даних та в cookies.

Реалізація скрипта check.php:

```
$link=mysqli_connect("localhost", "mysql_user", "mysql_password",
"authorization");

if (isset($_COOKIE["id"]) and isset($_COOKIE["hash"]))
{
$query = mysqli_query($link, "SELECT *, INET_NTOA(user_ip) AS user_ip FROM
users WHERE user_id = "".intval($_COOKIE["id"])."" LIMIT 1");
$userdata = mysqli_fetch_assoc($query);
if(($userdata["user_hash"]! == $_COOKIE["hash"]) or ($userdata["user_id"]!
== $_COOKIE["id"])
or (($userdata["user_ip"]! == $_SERVER["REMOTE_ADDR"]) and
($userdata["user_ip"]! == "0")))
{
setcookie("id", "", time() - 3600*24*30*12, "/");
setcookie("hash", "", time() - 3600*24*30*12, "/", null, null, true); //
httponly! !!
print "невдача";
}
else
{
print "Пиивіт, ".$userdata["user_login"]."! ";
}
}
else
```

```
{
print "Необхідно увімкнути cookies";
}
?>;
```

В скрипті перевірки здійснюється підключення до БД, хешований рядок та ідентифікаток користувача з бази даних порівнюються з такими ж змінними, які збереженні в cookie-файлі, в разі невдачі виводитися повідомлення про помилку, в протилежному випадку перевірка ввжається успшною.

Після цього був розроблений скрипт для самої авторизації. Користувач вводить свої логін та пароль у форму, після чого введенні дані порівнюються з даними в таблиці, в разі успішної перевірки користувач отримує доступ до ресурсу.

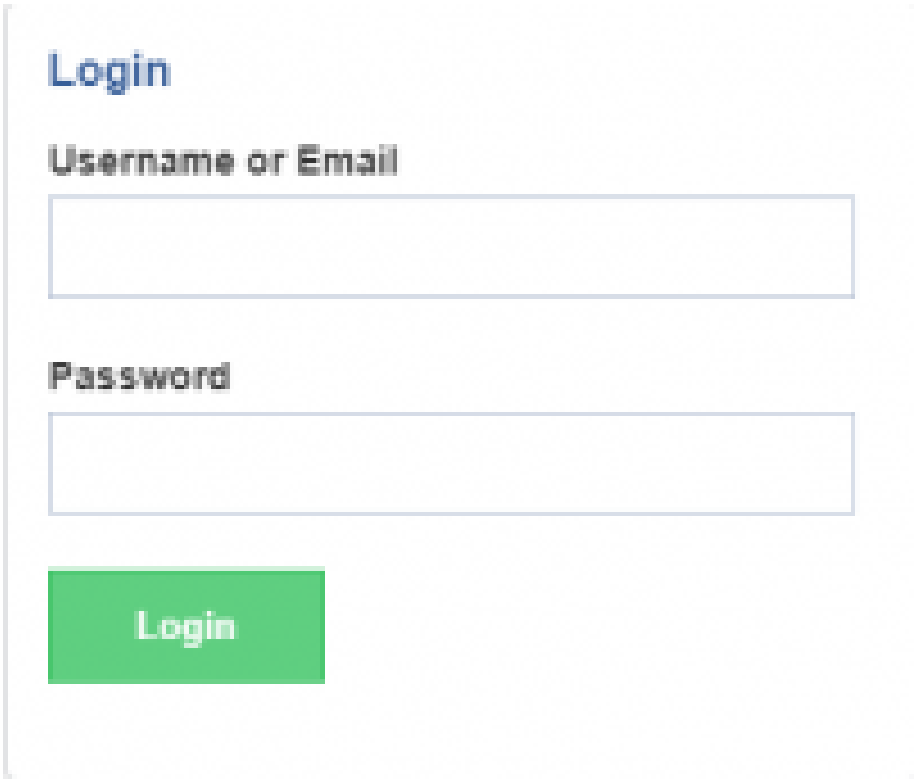


Рисунок 4.5 – форма авторизації

Скрипт авторизації звіряє введенний логін з логінами в базі даних, в разу успіху скрипт отримує запис з БД, в якому логін збігається з введеним. Після цього відбувається порівняння введенного паролю та розшифрованого паролю з бази даних, якщо вони збігаються користувач отримує доступ, якщо ні – користувач повинен авторизуватися повторно.

Останній скрипт призначений для розавторизації, в гому видаляються cookie файли та здійснюється вихіл з веб-сайту.

Реалізація logout.php:

```
<?
// Сторінка авторизації

// видалення кукі
setcookie("id", "", time() - 3600*24*30*12, "/");
setcookie("hash", "", time() - 3600*24*30*12, "/",null,null,true); // 
httponly !!!

// переадресація браузера
header("Location: /"); exit;

?>
```

4.3.3 Впровадження двофакторної автентифікації

Двофакторна авторизація використовується для підвищення захисту акаунтів користувачів від несанкціонованого доступу. Безліч людей використовують одні і ті ж зв'язки логін-пароль для доступу до різних сайтів, і це може бути використано зловмисниками.

Включення двофакторної авторизації на нашому сайті призведе до того, що то при кожному новому вході система буде додатково запитувати у користувача динамічний 6-значний код. Таким чином зловмисник, який заволодів логіном і паролем користувача, не зможе отримати доступ до цього аккаунту.

Динамічний код може бути отриманий різними способами, в даному випадку ми розглянемо використання програми Google Authenticator. Для

додавання двофакторної авторизації на сайт нам буде потрібно бібліотека GoogleAuthenticator.php.

1. Додаємо бібліотеку в наш проект (потрібні тільки 2 файли з дистрибутива):

```
FixedByteNotation.php
GoogleAuthenticator.php
```

2. Підключаємо клас Google Authenticator в наш скрипт:

```
require_once('GoogleAuthenticator.php');
```

3. Після того, як користувач перший раз включив двофакторну авторизацію необхідно обчислити і зберегти його секретний ключ. Цей секретний ключ використовується для генерації та перевірки динамічних кодів:

```
$ga=new GoogleAuthenticator;
$user->ga_secret=$ga->generateSecret();
$user->save();
```

4. Коли отримано секретний ключ слід показати користувачеві інструкцію по установці програми Google Authenticator (можна скористатися інструкцією від Google). Також буде потрібно вивести QR-code-це дозволить легко додати ключ для нашого сайту в програму Google Authenticator. Розумним рішенням також є введення перевірочного коду, це служить сигналом що користувач успішно встановив програму і для нього можна включати другий фактор авторизації. Для показу QR-коду можна скористатися методом getUrl класу Google Authenticator:

```
$ga=new GoogleAuthenticator;
$ga->getUrl($user->login,'mysite.com',$user-
>ga_secret);
```

5. Перевірка введеного в авторизаційну форму секретного коду:

```
$ga=new GoogleAuthenticator;
$code=$ga->getCode($user->ga_secret);
if ($code!=$_POST['code']) return new
AuthError('invalid code');
```

Змінна $ code повинна відповідати введеному Користувачем у форму входу.

4.4 Висновки

В цьому розділі було розробленно програмне забезпечення для авторизації доступу на основі ролей. В першу чергу була розроблена база даних для зберігання даних необхідних для авторизації та даних, які стосуються ролей та повноважень, що ними надаються, інструментом для цього слугувала мова запитів SQL та веб-сайт для керування базами даних phpmyadmin.com. Потім розроблемно систему авторизації доступу та контролю доступу на основі ролей за допомогою мови програмування PHP.

ВИСНОВКИ

Інформація завжди була важливим ресурсом проте в час стрімкого розвитку технологій її цінність зростає з кожним днем, а це говорить лише про одне – інформація потребує серйозного захисту, як і будь-який цінний ресурс.

Несанкціонований доступ являється однією з найголовніших загроз інформації. З розвитком технологій в кібератаках стають зацікавленими все більше сторін: від звичайних ентузіастів до потужних угрупувань та кібервійськ з необмеженими ресурсами. В таких реаліях постає проблема захисту інформації від несанкціонованого досутупу, що і є завданням кваліфікаційної роботи.

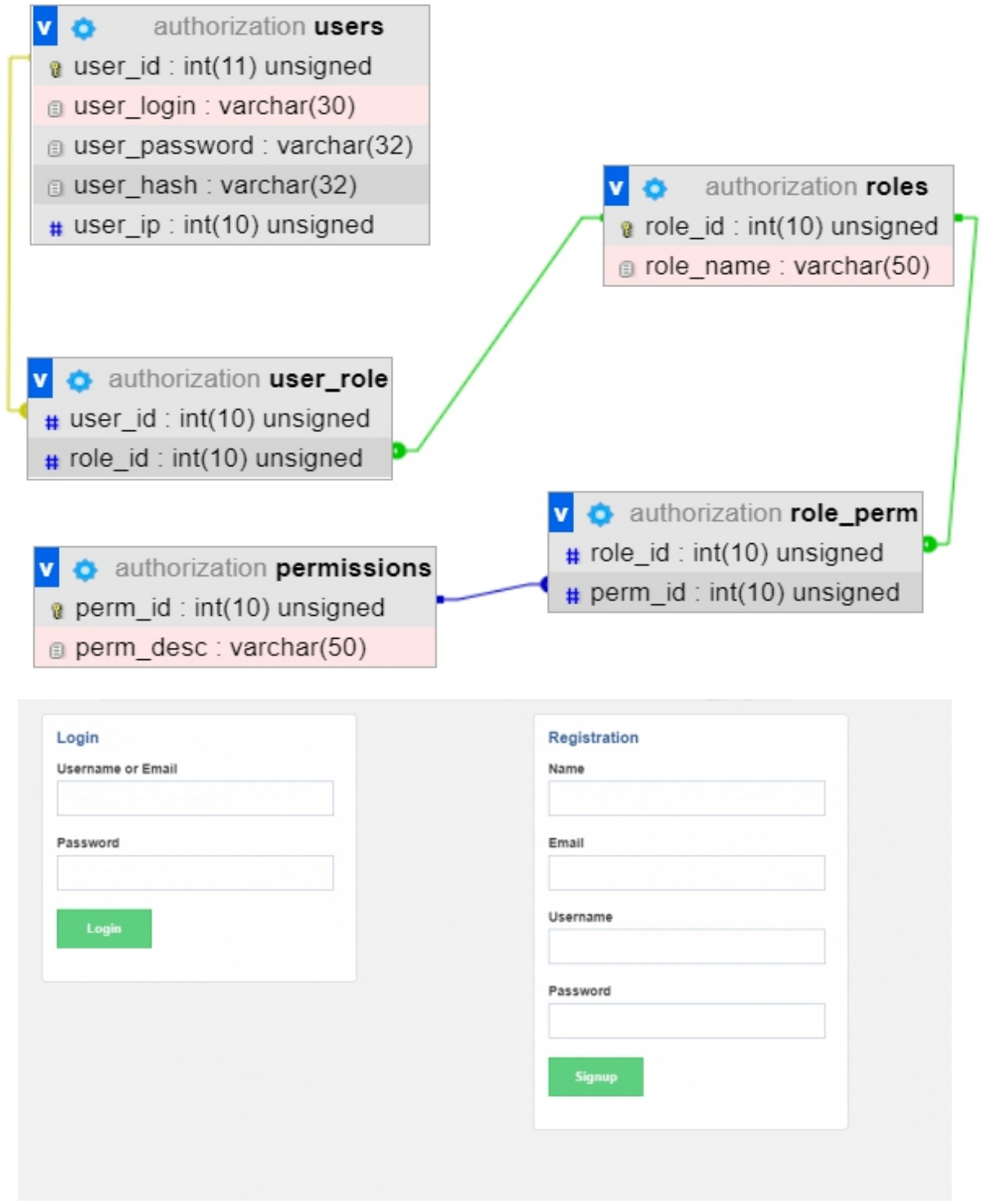
Згідно з завданням, в ході виконання кваліфікаційної роботи було проведенно ознайомлення з поняттями в галузі захисту від НСД, оглянуто сучасні розробки. В ході роботи було розглянуто особливості діяльності підприємства, вивчено його структуру. Після чого було розроблемно ситему авторизації доступу за методом рольового контролю доступу та впроваджено двофакторну автентифікацію для забезпечення максимального рівня безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

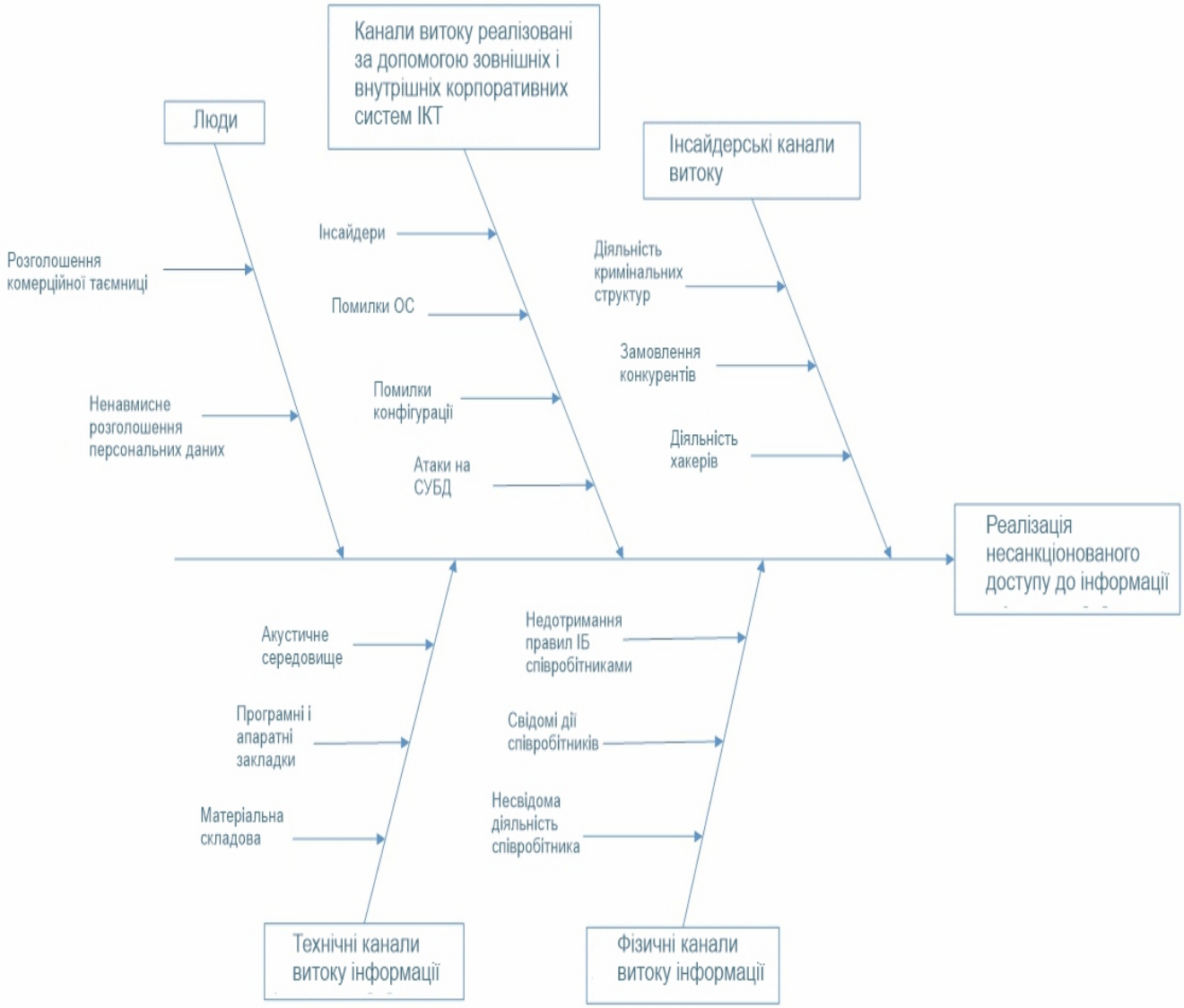
1. Itglobal.com [Електронний ресурс]. - Електронні дані. – Режим доступу: www.itglobal.com(дата звернення 24.04.2021). - Назва з екрану.
2. Ifac.org [Електронний ресурс]. - Електронні дані. - Режим доступу: www.ifac.org(дата звернення 27.04.2021). - Назва з екрану
3. hubr.com [Електронний ресурс]. - Електронні дані - Режим доступу: www.hubr.com (дата звернення 12.05.2021). - Назва з екрану
4. cybersecurity.springeropen.com [Електронний ресурс]. – Електронні дані - Режим доступу: www. cybersecurity.springeropen.com (дата звернення 21.04.2021). - Назва з екрану
5. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
6. Система забезпечення інформаційної безпеки України // Національна безпека і оборона. - 2001. - № 1. - С. 16-28
7. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский,; Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій. -Одеса, 2001. -164 с.
8. Бондарь И. Проблемы информационной безопасности в условиях переходного общества // Персонал. - 2003. - № 8. - С. 47-48.
9. Karp A., Haury H., and Davis M. From ABAC to ZBAC: The evolution of access control models // ISSA J. 2010.
10. Ferraiolo, D., Kuhn, D.R., Chandramouli, R. 2007. Rolebased Access Control. Artech House Inc.
11. Daniel Servos, Sylvia L. Osborn. Current Research and Open Problems in AttributeBased Access Control. – 2017.

ДОДАТОК А
(Обов’язковий)

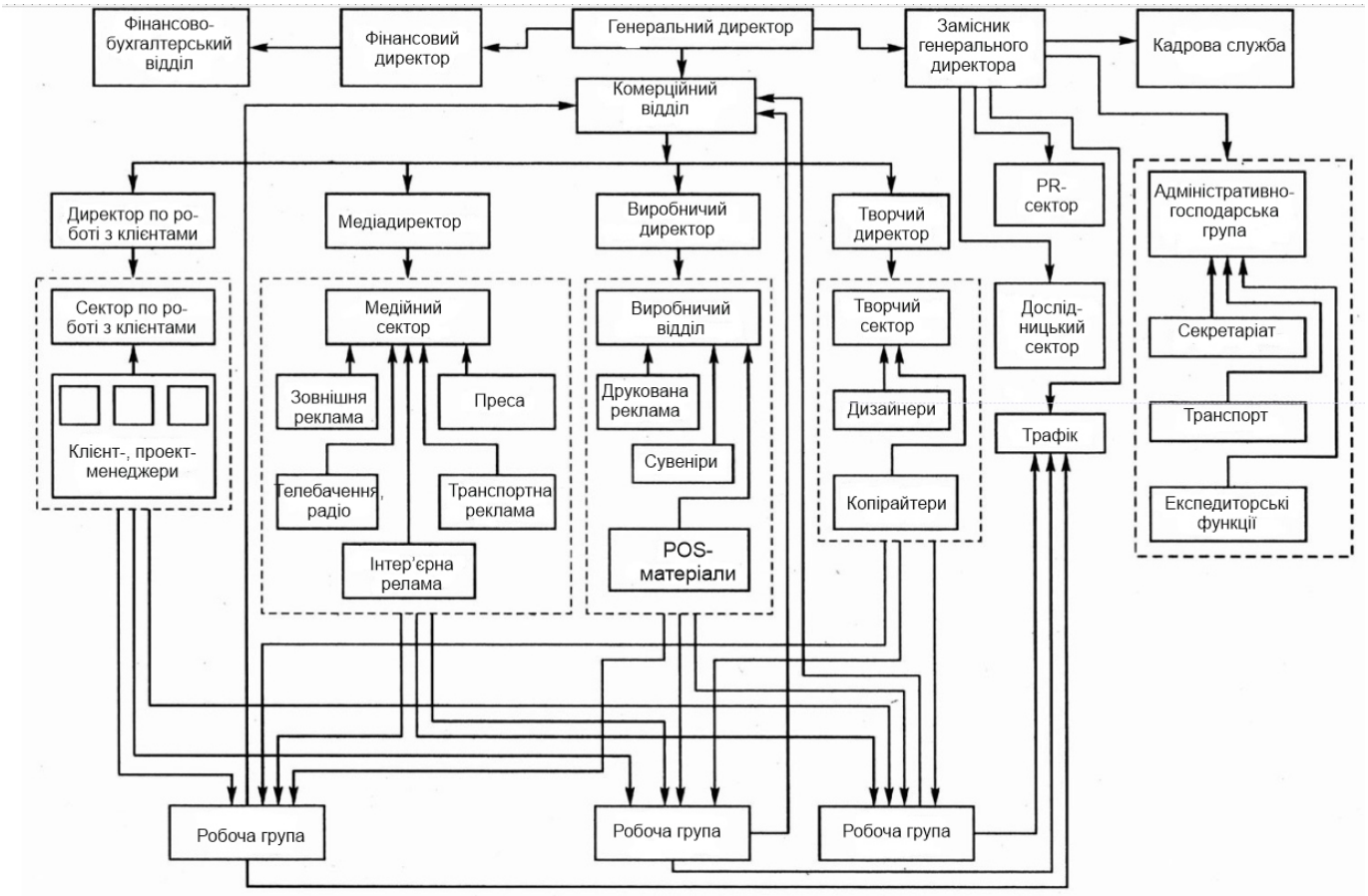
Копія графічної частини



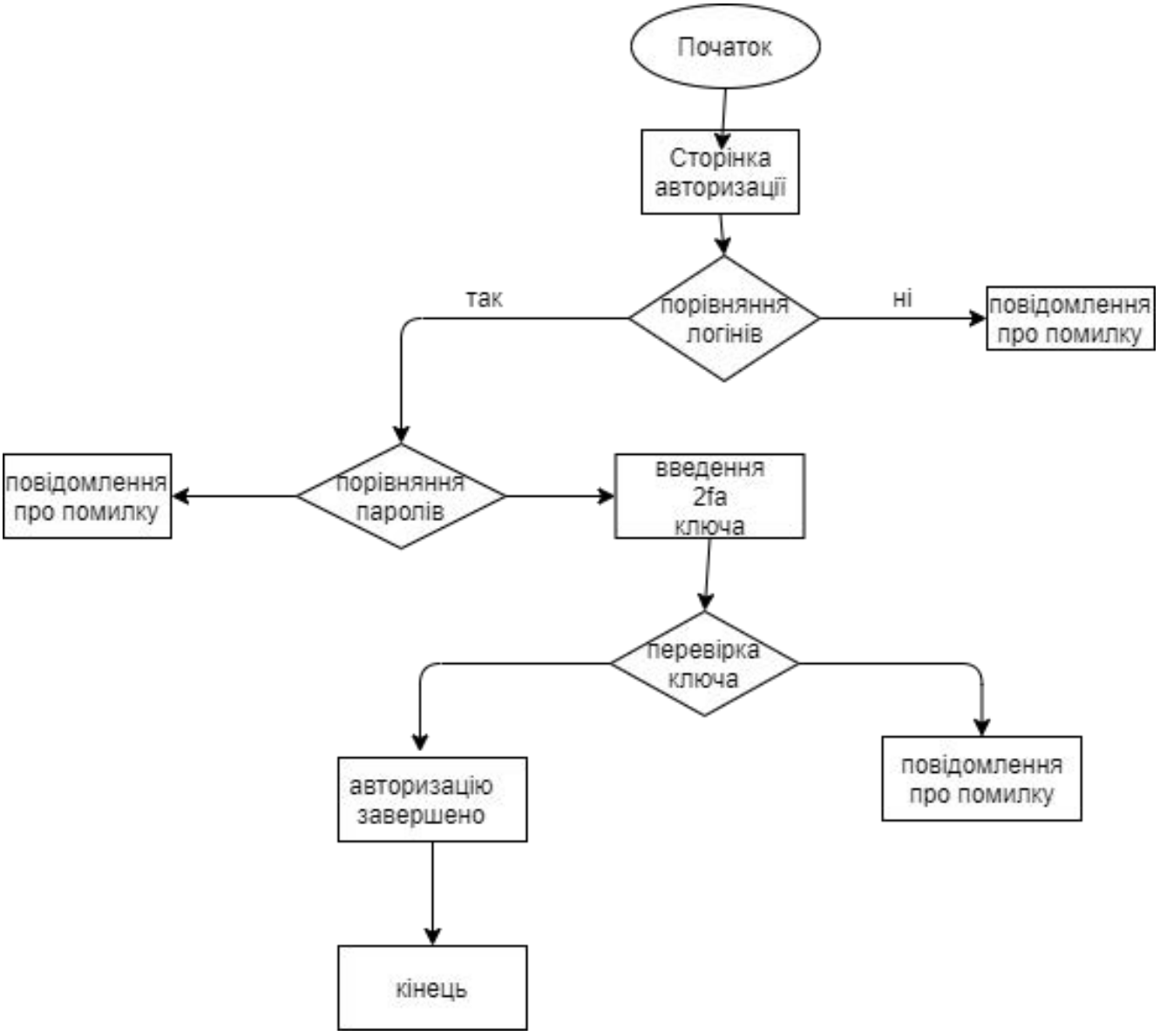
					КПКБ.170151.17.01.12 Е8		
					Зв’язок бази даних з формами	Літера	Маса / Масштаб
Зм.	Арк.	№ документа	Підпис	Дата			
Розроб.		Пенцак Р.О.					
Перевір.		Орленко В.С.				Аркуш	Аркушів
Н.контр.							
Т.контр.		Муляр І.В.				ХНУ КБ-17-1	
Затверд.		Кльоц Ю.П.					



					КПКБ.170151.17.01.12 Е8	
Зм.	Арк.	№ документа	Підпис	Дата	Модель загроз інформаційній безпеці	Літера / Маса / Масштаб
Розроб.		Пенцак Р.О.				
Перевір.		Орленко В.С.				Аркуш / Аркушів
Н.контр.						
Т.контр.		Муляр І.В.			ХНУ КБ-17-1	
Затверд.		Кльоц Ю.П.				



					КПКБ.170151.17.01.12 Е8	
Зм.	Арк.	№ документа	Підпис	Дата	Структура підприємства	Літера / Маса / Масштаб
Розроб.		Пенцак Р.О.				
Перевір.		Орленко В.С.				Аркуш / Аркушів
Н.контр.						
Т.контр.		Муляр І.В.				ХНУ КБ-17-1
Затверд.		Кльоц Ю.П.				



					КПКБ.170151.17.01.12 Е8	
						Літера / Маса / Масштаб
Зм.	Арк.	№ документа	Підпис	Дата	Авторизація з використанням 2FA	
Розроб.		Пенцак Р.О.				Аркуш / Аркушів
Перевір.		Орленко В.С.				
Н.контр.						
Т.контр.		Муляр І.В.				ХНУ КБ-17-1
Затверд.		Кльоц Ю.П.				

ДОДАТОК Б
(Обов'язковий)

Програмна реалізація

```
<?php
class Role
{
    protected $permissions;

    protected function __construct() {
        $this->permissions = array();
    }

    // повертаємо об'єкт ролі з відповідними повноваженнями
    public static function getRolePerms($role_id) {
        $role = new Role();
        $sql = "SELECT t2.perm_desc FROM role_perm as t1
                JOIN permissions as t2 ON t1.perm_id = t2.perm_id
                WHERE t1.role_id = :role_id";
        $sth = $GLOBALS["DB"]->prepare($sql);
        $sth->execute(array(":role_id" => $role_id));

        while($row = $sth->fetch(PDO::FETCH_ASSOC)) {
            $role->permissions[$row["perm_desc"]] = true;
        }
        return $role;
    }

    // перевірка встановлених повноважень
    public function hasPerm($permission) {
        return isset($this->permissions[$permission]);
    }
// Додати в таблицю нову роль
public static function insertRole($role_name) {
    $sql = "INSERT INTO roles (role_name) VALUES (:role_name)";
    $sth = $GLOBALS["DB"]->prepare($sql);
    return $sth->execute(array(":role_name" => $role_name));
}

// Додати масив ролей для вказаного користувача
public static function insertUserRoles($user_id, $roles) {
    $sql = "INSERT INTO user_role (user_id, role_id) VALUES (:user_id,
:role_id)";
    $sth = $GLOBALS["DB"]->prepare($sql);
    $sth->bindParam(":user_id", $user_id, PDO::PARAM_STR);
    $sth->bindParam(":role_id", $role_id, PDO::PARAM_INT);
    foreach ($roles as $role_id) {
        $sth->execute();
    }
    return true;
}

// видалити масив ролей та усі зв'язки цього масиву
public static function deleteRoles($roles) {
    $sql = "DELETE t1, t2, t3 FROM roles as t1
            JOIN user_role as t2 on t1.role_id = t2.role_id
            JOIN role_perm as t3 on t1.role_id = t3.role_id
            WHERE t1.role_id = :role_id";
    $sth = $GLOBALS["DB"]->prepare($sql);
    $sth->bindParam(":role_id", $role_id, PDO::PARAM_INT);
```

```
    foreach ($roles as $role_id) {
        $sth->execute();
    }
    return true;
}

// видали масив ролей для вказаного користувача
public static function deleteUserRoles($user_id) {
    $sql = "DELETE FROM user_role WHERE user_id = :user_id";
    $sth = $GLOBALS["DB"]->prepare($sql);
    return $sth->execute(array(":user_id" => $user_id));
}

}

<?php
class PrivilegedUser extends User
{
    private $roles;

    public function __construct() {
        parent::__construct();
    }

    // метод для отримання об'єкту з ролями та повноваженнями користувача або
його створення, якщо користувач не наділений повноваженнями
    public static function getByUsername($username) {
        $sql = "SELECT * FROM users WHERE user_id = :user_id";
        $sth = $GLOBALS["DB"]->prepare($sql);
        $sth->execute(array(":user_id" => $user_id));
        $result = $sth->fetchAll();

        if (!empty($result)) {
            $privUser = new PrivilegedUser();
            $privUser->user_id = $result[0]["user_id"];
            $privUser->user_login = $result[0]["user_login"];
            $privUser->user_password = $result[0]["user_password"];
            $privUser->user_hash = $result[0]["email_addr"];
            $privUser->user_ip = $result[0]["user_ip"];
            $privUser->initRoles();
            return $privUser;
        } else {
            return false;
        }
    }

    // метод для наповнення ролей необхідними повноваженнями
    protected function initRoles() {
        $this->roles = array();
        $sql = "SELECT t1.role_id, t2.role_name FROM user_role as t1
                JOIN roles as t2 ON t1.role_id = t2.role_id
                WHERE t1.user_id = :user_id";
        $sth = $GLOBALS["DB"]->prepare($sql);
        $sth->execute(array(":user_id" => $this->user_id));

        while($row = $sth->fetch(PDO::FETCH_ASSOC)) {
            $this->roles[$row["role_name"]] =
Role::getRolePerms($row["role_id"]);
        }
    }

    // перевірка користувача на наявність повноважень
    public function hasPrivilege($perm) {
        foreach ($this->roles as $role) {
            if ($role->hasPerm($perm)) {
                return true;
```

```
            }
        }
        return false;
    }
// перевірка користувача на наявність певної ролі
public function hasRole($role_name) {
    return isset($this->roles[$role_name]);
}

// додавання нового повноваження в роль
public static function insertPerm($role_id, $perm_id) {
    $sql = "INSERT INTO role_perm (role_id, perm_id) VALUES (:role_id,
:perm_id)";
    $sth = $GLOBALS["DB"]->prepare($sql);
    return $sth->execute(array(":role_id" => $role_id, ":perm_id" => $perm_id));
}

// видалення повновадень з ролі
public static function deletePerms() {
    $sql = "TRUNCATE role_perm";
    $sth = $GLOBALS["DB"]->prepare($sql);
    return $sth->execute();
}

}



<?

// сторінка реєстрації

// з’єднання з БД

$link=mysqli_connect("localhost", "mysql_user", "mysql_password",
"autorization");



if(isset($_POST['submit']))

{

    $err = [];

    // перевірка логіну

    if(!preg_match("/^[a-zA-Z0-9]+$/",$_POST['login']))

    {

        $err[] = "Логін може містити лише цифри та латинські букви";

    }



    if(strlen($_POST['login']) < 3 or strlen($_POST['login']) > 30)

    {

        $err[] = "Довжина логіну від 3 до 30 символів!";

    }
```

```
    // перевіряємо, чи не існує такого користувача

    $query = mysqli_query($link, "SELECT user_id FROM users WHERE
user_login='".mysqli_real_escape_string($link, $_POST['login'])."'");

    if(mysqli_num_rows($query) > 0)

    {

        $err[] = "Користувач з таким іменем існує!";

    }


    // Якщо помилок немає – додаєм користувача в БД

    if(count($err) == 0)

    {


        $login = $_POST['login'];


        // забираємо зайві пробіли та проводимо подвійне хешування

        $password = md5(md5(trim($_POST['password'])));


        mysqli_query($link,"INSERT INTO users SET user_login='".$login."',
user_password='".$password."'");

        header("Location: login.php"); exit();

    }

    else

    {

        print "<b>При реєстрації виникли наступні помилки:</b><br>";

        foreach($err AS $error)

        {

            print $error."<br>";

        }

    }

}

?>


<form method="POST">

Логін <input name="login" type="text" required><br>
```

```
Пароль <input name="password" type="password" required><br>

<input name="submit" type="submit" value="S ">

</form>



<?

// скрипт перевірки



// з’єднання з БД

$link=mysqli_connect("localhost", "mysql_user", "mysql_password",
"authorization");



if (isset($_COOKIE['id']) and isset($_COOKIE['hash']))

{

    $query = mysqli_query($link, "SELECT *,INET_NTOA(user_ip) AS user_ip FROM
users WHERE user_id = '".intval($_COOKIE['id'])."' LIMIT 1");

    $userdata = mysqli_fetch_assoc($query);



    if(($userdata['user_hash'] !== $_COOKIE['hash']) or ($userdata['user_id']
!== $_COOKIE['id'])

 or (($userdata['user_ip'] !== $_SERVER['REMOTE_ADDR'])  and
($userdata['user_ip'] !== "0")))

    {

        setcookie("id", "", time() - 3600*24*30*12, "/");

        setcookie("hash", "", time() - 3600*24*30*12, "/", null, null, true); //
httponly !!!

        print "невдача";

    }

    else

    {

        print "ПРивіт, ".$userdata['user_login']."!";

    }

}

else

{

    print "Необхідно увімкнути cookies";
```

```
}

?>

<?

// сторінка авторизації


// функція для генерації випадкового рядка

function generateCode($length=6) {

    $chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHI JKLMNOPRQSTUVWXYZ0123456789";

    $code = "";

    $clen = strlen($chars) - 1;

    while (strlen($code) < $length) {

            $code .= $chars[mt_rand(0,$clen)];

    }

    return $code;

}


// з’єднання з БД

$link=mysqli_connect("localhost", "mysql_user", "mysql_password",
"authorization");


if(isset($_POST['submit']))

{

    // отримуємо з БД запис, в якому логін збігається з введеним

    $query = mysqli_query($link,"SELECT user_id, user_password FROM users WHERE
user_login='".mysqli_real_escape_string($link,$_POST['login'])."' LIMIT 1");

    $data = mysqli_fetch_assoc($query);


    // зрівнюємо паролі

    if($data['user_password'] === md5(md5($_POST['password'])))

    {

        // генеруємо впад=лкове число та хешуємо його

   $hash = md5(generateCode(10));


     if(!empty($_POST['not_attach_ip']))
```

```
        {
            // якщо користувач вибрав прив’язку до IP
            // переводимо ip в рядок
            $insip = ", user_ip=INET_ATON('".$_SERVER['REMOTE_ADDR']."')";
        }

        // записуємо в БД новий хеш авториації та IP
        mysqli_query($link, "UPDATE users SET user_hash='".$hash."' ".$insip."
WHERE user_id='".$data['user_id']."'");

        // встановлюємо cookies
        setcookie("id", $data['user_id'], time()+60*60*24*30, "/");
        setcookie("hash", $hash, time()+60*60*24*30, "/", null, null, true); //
httponly !!!

        // переадресовуємо браузер на перевірку
        header("Location: check.php"); exit();
    }
    else
    {
        print "ви ввели неправильний логін або пароль";
    }
}
?>
<form method="POST">
Логін <input name="login" type="text" required><br>
Пароль <input name="password" type="password" required><br>
Не прикріпляти до IP(менш безпечно) <input type="checkbox"
name="not_attach_ip"><br>
<input name="submit" type="submit" value="Увійти">
</form>
<?
// Сторінка авторизації
```

```
// видалення кукі

setcookie("id", "", time() - 3600*24*30*12, "/");

setcookie("hash", "", time() - 3600*24*30*12, "/",null,null,true); // httponly
!!!


// переадресація браузера

header("Location: /"); exit;


?>

<form method="POST">

    Логін <input name="login" type="text" required><br>

    Пароль <input name="password" type="password" required><br>

    Не прикріпляти до IP(менш безпечно) <input type="checkbox"
name="not_attach_ip"><br>

    <input name="submit" type="submit" value="увійти">

</form>
```

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Забезпечення реалізації процесів попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації доступу до каналів передачі даних телекомунікаційної системи рекламного агентства

Автор: Пенцак Роман Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Керівник: Орленко Вікторія Сергіївна, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

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

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 4.31% що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В.С. Орленко

Завідувач кафедри КбКСМ, гарант ОП _____ Ю.П. Кльоц

Дата: 16.06.2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Пенцак Роман Олександрович

Тема Забезпечення реалізації процесів попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації доступу до каналів передачі даних телекомунікаційної системи рекламного агентства

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 58.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано систему авторизації та розмежування доступу.

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

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено предмет та об'єкт дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено аналіз існуючих рішень та методів протидії отримання несанкціонованого доступу на етапі попередження, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі наведені засоби та методи використані для побудови системи авторизації та розмежування доступу. В третьому розділі було проведено аналіз діяльності підприємства, його структуру та потоки цінної інформації . У четвертому розділі була проведена розробка програмного забезпечення яке реалізує функціонал, необхідний для авторизації та розмежування доступу до телекомунікаційних мереж.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність полягає у розробці програмного забезпечення, яке забезпечує безпечну авторизацію в межах телекомунікаційної мережі підприємства.

5. Негативні сторони роботи Розроблена система авторизації доступу володіє недостатнім функціоналом.

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

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

8. Інші зауваження в ході виконання роботи приведено мало прикладів роботи програми, що не дозволяє скласти цілковитого уявлення про роботу програми

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

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Говорущенко Т. О., завідувач каф. КІСП, д. т. н., професор

« ____ » _____ 2021. _____ (підпис)

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008314208

Check date:
16.06.2021 18:42:35 EEST

Check type:
Doc vs Internet

Report date:
16.06.2021 18:43:17 EEST

User ID:
100005590

File name: **КвРКБ_Пенцак**

Page count: **58** Word count: **10196** Character count: **83970** File size: **1.33 MB** File ID: **1008381528**

4.31% Matches

Highest match: **1.16%** with Internet source (http://ir.nmu.org.ua/bitstream/handle/123456789/151306/%D0%A1%D1%82%D0%B0%

4.31% Internet sources | 26 ..... Page 60

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters | 9

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 94370 Название: Попередження отриманню несанкціонованого доступу та впровадження заходів по здійсненню авторизації Добавлено в БД: 2021-06-16 Авторы: Пенцак Р.О. Руководители: Орленко В.С. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	71071	612	1142 (2%)	14 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы