МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____2021 р.

На правах рукопису
УДК 004.056:004.738.5(079.2)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система контролю доступу до персональних даних

Виконавець: М.В. Скрипка
Керівник: к.т.н., доцент М.Б. Гумен
Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____2021 р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Скрипки Максима Вікторовича

1. Тема: *Система контролю доступу до персональних даних*
затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати характерні ознаки персональних даних та визначити їх відмінності від інших видів інформації; дослідити методи контролю доступу до персональних даних; розробити систему контролю доступу web-сайту компанії.
4. Зміст пояснювальної записки: аналіз видів інформації і персональних даних; дослідження методів та основних компонентів контролю доступу; розробка системи контролю доступу web-сайту компанії, обґрунтування заходів щодо організації захисту інформаційної системи обробки персональних даних.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	10.05.2021	*Виконано*
2.	Аналіз літературних джерел	11.05.2021-14.05.2021	*Виконано*
3.	Обґрунтування вибору рішення	15.05.2021-17.05.2021	*Виконано*
4.	Збір інформації	18.05.2021-22.05.2021	*Виконано*
5.	Дослідження існуючих систем контролю доступу до персональних даних	23.05.2021-24.05.2021	*Виконано*
6.	Дослідження сучасних методів захисту інформації	25.05.2021-28.05.2021	*Виконано*
7.	Обґрунтування заходів щодо організації захисту інформаційної системи обробки персональних даних.	29.05.2021-02.06.2021	*Виконано*
8.	Розробка системи контролю доступу web-сайту компанії	03.06.2021	*Виконано*
9.	Перевірка на антиплагіат	04.06.2021-06.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	07.06.2021-08.06.2021	*Виконано*
11.	Оформлення презентації	09.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	11.06.2021	*Виконано*

Здобувач вищої освіти _____ М.В. Скрипка
(підпис, дата)

Керівник дипломної роботи _____ М.Б. Гумен
(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 66 сторінки, має 13 рисунків. Список використаних джерел містить 39 найменувань і займає 2 сторінки.

Метою дипломної роботи є розробка системи контролю доступу до персональних даних.

В роботі розглянуто сукупність методів, заходів і засобів для запобігання несанкціонованого доступу до ресурсів, для забезпечення цілісності даних. Були проаналізовані методи і засоби шифрування даних, те як можна авторизуватись за допомогою SSH протоколу, захистити персональні дані за допомогою двофакторної автентифікації та як можна авторизуватись через фізичний USB-ключ носій.

В результаті проведеної роботи створено модель системи контролю безпеки даних на прикладі створення ресурсу - сайту інтернет магазину.

Ключові слова: персональні дані, контроль доступу, система контролю управління доступом, двофакторна автентифікація, USB-ключ доступу.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ACS - Access Control System (контрольована система доступу)

CRUD – Create Read Update Delete

DFD - Data Flow Diagrams (діаграма потоків даних)

ER diagram – Entity Relationship diagram

GDPR - General data protection regulation (загальний регламент захисту даних)

SSL – Secure Sockets Layer (рівень захищених сокетів).

SIEM - Security information and event management

SIM - Security information management (управління подіями безпеки)

SSH - Secure Shell (мережевий протокол рівня застосунків)

SQL – Structure Query Language (структурована мова записів)

TCP – Transmission Control Protocol (протокол керування передачею).

IP – Internet Protocol

NF – Normal Forms

USB - Universal Serial Bus

БД – база даних

ІКТ – інформаційно-комунікаційні технології

ІТ – інформаційні технології.

НСД – несанкціонований доступ

ОС – операційна система

СКД – система контролю даних

СКУД – система контролю управління даними

СУБД – система управління базою даних

СЗ – система захисту

ВСТУП

Актуальність. З кожним днем сучасні технології розвиваються ще більш стрімкішими темпами, а тому розробникам доводиться шукати нові способи якісного захисту інформаційних технології. Якщо ще зовсім недавно використовувалися лише засоби захисту з обмеженою функціональністю, то вже сьогодні існують різні міжмережні екрани наступного покоління, системи виявлення різних вторгнень і багато інших систем, що дозволяють більшою мірою здійснювати якісний захист.

Діяльності майже кожного підприємства притаманна робота з інформацією про людей. Обробляються дані про співробітників компанії, партнерів, акціонерів і т. д. Вся інформація, що відноситься до прямо або побічно визначеної або визначеної фізичної особи, згідно чинного законодавства встановлено вимоги щодо захисту персональних даних при їх обробці в інформаційних системах.

Таким чином, актуальність цієї роботи обумовлена необхідністю організації захисту інформаційної системи обробки персональних даних.

Персональні дані – це будь-яка інформація, що відноситься до прямо або побічно визначеної або невизначеної фізичної особи (суб'єкта персональних даних).

Безсумнівно, персональні дані відіграють дуже важливу роль для кожного з нас. При прийомі на роботу, а також при укладанні трудового договору кожен працівник отримує інформацію про потенційного свого роботодавця, в тому числі про місце його фактичного перебування та про характер своєї майбутньої роботи. Але, крім того, величезне значення знання персональних даних працівника має і для роботодавця, він теж отримує інформацію про даного працівника, про його вік, професію, спеціалізацію, кваліфікацію, стан здоров'я, сімейний стан і про багато іншого. Вся ця інформація дуже потрібна роботодавцю, адже вона витікає не тільки з трудового, а й з цивільного, сімейного, адміністративного, інших галузей законодавства (наприклад, для утримання із заробітної плати податків, коштів у відшкодування шкоди, аліментів), для надання праців-

нику пільг і переваг, наприклад, при переведенні на іншу роботу у зв‘язку з хворобою, вагітністю, на сьогоднішній день роботодавцю дано право отримувати всю необхідну інформацію про персональні дані працівника, але в той же час законодавство зобов‘язує його вживати всіх заходів для попередження несанкціонованого виходу цієї інформації з ведення роботодавця, щоб персональні дані працівника не стали надбанням третіх осіб без його відома та згоди. В цілому, регулюванню та забезпеченню конфіденційності персоніфікованої інформації про працівників, присвячені норми, які містяться в статтях закону про захист персональних даних працівника.

Сучасні інформаційні системи підприємств і організацій, поряд зі зберіганням і обробкою ділової інформації, вирішують завдання зберігання і обробки ПД співробітників і контрагентів. Це тягне за собою необхідність організації обробки та захисту ПД відповідно до вимог чинного законодавства в даній галузі.

Захист ПД є одним з найважливіших завдань системи забезпечення інформаційної безпеки в організації будь-якого масштабу і будь-якої організаційно-правової форми господарювання.

Актуальність роботи обумовлена також тим, що оператор зобов‘язаний виконувати вимоги законодавства щодо персональних даних, але при організації захисту ПДН в СПД він стикається з труднощами щодо врахування вимог великої кількості нормативних документів, що регламентують процес побудови СЗПД.

Метою роботи є розробка системи контролю доступу до персональних даних для забезпечення інформаційної безпеки підприємства за рахунок мінімізації витрат і підвищення ефективності.

Для досягнення мети роботи необхідно виконати наступні **завдання:**

- проаналізувати характерні ознаки персональних даних та визначити їх відмінності від інших видів інформації;
- простежити розвиток законодавства в галузі контролю доступу до персональних даних;

- дослідити методи та засоби контролю управління доступом персональних даних, виявити їх недоліки та переваги;
- розробити систему контролю доступу web-сайту компанії.

Поставлені мета та завдання досягаються за допомогою таких методів дослідження як вивчення документів, нормативно-правових актів, порівняльного аналізу, спостереження, узагальнення.

Об'єкт дослідження: процес контролю та управління доступом до персональних даних

Предмет дослідження: засоби та методи контролю та управління доступом.

Практична цінність роботи полягає у розробці системи контролю доступу до персональних даних на прикладі сайту інтернет магазину з визначенням рівня доступу і контрольованого надання інформації. Наявність у розробленій системі підсистем шифрування md5 з додаванням спеціального набору символів, CRUD (Створення Читання Редагування Видалення) та щоденного резервного копіювання ресурсу робить процеси отримання і обробки даних надійними та забезпечує безперервність роботи сайту і прискорення відновлення даних.

Галузь застосування. Дана робота може бути використання під час розробки веб-сайтів при обранні методів захисту.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ПИТАННЯ КОНТРОЛЮ ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Основні поняття контролю доступу до персональних даних

1.1.1 Поняття персональних даних

На сьогоднішній день основні процеси життєдіяльності людини не можуть існувати без персонального дозволу і надання особистої інформації державним органам, іншим членам суспільства, громадським організаціям. У ст. 2 Закону України «Про інформацію» від 02.10.1992 р. повідомляється, що кожна людина має право вільного отримання інформації, її поширення, зберігання, захисту і використання в межах своїх прав, свобод та законних інтересів [1]. Згідно до Закону України «Про захист персональних даних», персональні дані — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. За порушення законодавства та встановленого порядку захисту персональних даних та інформації, що спричинило надання незаконного доступу або порушення прав пацієнтів як суб’єктів персональних даних, відповідальна особа може бути притягнута до адміністративної відповідальності.

Сьогодні до захисту конфіденційної інформації висувають все жорсткіші вимоги. Оскільки особисті дані людей містять персональний характер, до забезпечення гарантій щодо їх захисту і нерозповсюдження відносяться серйозно. У зв'язку з цим документація, що регулює забезпечення захисту персональних даних людей, зокрема працівників, передбачені не тільки у національному законодавстві, а й міжнародними законами.

Стаття 12 Загальної декларації прав людини 1948 року свідчить «Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя. Ко-

жна людина має право на захист закону від такого втручання або таких посягань». Право на повагу до приватного і сімейного життя міститься так само і в Конвенції про захист прав людини і основних свобод. Ці міжнародні правові акти заклали основу створення національних правових систем. Необхідно відзначити, що приймалися вони через кілька років після руйнівної Світової війни, в той час, коли права людини були чимось дуже далеким від реальності. І, тим не менше, право недоторканності приватного життя (в тому числі конфіденційних відомостей) було вписано в Декларацію як одне з основних [2]

1.1.2 Поняття контролю доступу

Контроль доступу - це функція відкритої системи, яка забезпечує технологію захисту, яка дозволяє чи забороняє доступ до різних типів інформації, що базується на ідентифікації суб'єкта, котрому потрібен доступ, і об'єкта даних, що є метою доступу” [3].

Вибір методу контролю доступу визначається політикою інформаційної безпеки компанії. Неструктуровані дані повинні бути розділені на групи з різним рівнем конфіденційності. Разом з цим певні права надаються окремим користувачам або групам користувачів, далі вибір моделі контролю залежить від архітектури інформаційної системи. Чимало організацій, окрім встановлення різного рівня прав доступу до неструктурованої інформації на програмному рівні, використовують апаратні засоби, які ускладнюють несанкціоноване застосування комп'ютера або вхід до інформаційної системи. До таких засобів відносяться токени та інші технічні засоби ідентифікації.

Програмні засоби дають можливість співвіднести права користувача і важливість об'єкта. На ринку представлено кілька продуктів, що дозволяють зберегти неструктуровані дані від розкриття. Системи Data Access Governance і Data-Centric Audit and Protection відстежують активність співробітників в інформаційних системах та визначають, хто, коли і з яким файлом взаємодіяв. Знання про наявність програм обліку та фіксації операцій з об'єктами лімітованого

доступу дисциплінує співробітників, вони розуміють, що їх некоректні дії будуть виявлені. Дані систем стають доказом не тільки при проведенні внутрішнього розслідування витоків, але і для судів і правоохоронних органів. Мінусом стає те, що програміст або системний адміністратор можуть видалити відомості про операції з неструктурованою інформацією обмеженого доступу.

Система контролю доступу збирає, записує та обробляє великі обсяги особистих даних. Деякі дані можуть бути вразливими. Наприклад, ім'я власника картки (суб'єкта даних), номер працівника, PIN-код, ідентифікаційні фотографії та кадри відеоспостереження. А також системи контролю доступу фіксують рух власників даних. На основі цієї інформації є можливість здійснювати контроль за поведінкою людини. Суб'єкти даних часто не мають уявлення про особисті дані, які контролюються системами контролю доступу, як довго вони зберігаються, чи зберігаються вони надійно, де і кому вони надаються.

Захист особистих даних суб'єктів часто залишається поза увагою, тому його досить легко порушити. Наприклад, системний адміністратор часто може перевіряти транзакції контролю доступу всіх власників карток. Цим правом можна зловживати, використовуючи інформацію в цілях, що не стосуються захисту. Відповідно до GDPR це буде класифіковано як "порушення даних".

General data protection regulation (GDPR) - це загальний регламент захисту даних, який з 25 травня 2018 року контролює збір, уніфікацію і використання персональних даних в країнах ЄС. З метою забезпечення відповідності контролю доступу до даних вимогам GDPR, потрібно більше зосередитися на безпеці даних. Це слід розглядати на етапі проектування, особливо доступ до даних, їх редагування та видалення.

1.1.3 Типи контролю доступу

У випадку, якщо безпека є важливою ланкою для офісу, система контролю доступу є обов'язковим атрибутом компанії. СКУД дозволить прохід довіреним персонам, та не дозволить увійти невідомим. Також є можливість налагодити

доступ до кабінетів у офісі. Контроль доступу - це помічник, котрий надає доступ лише перевірених працівників до різних областей компанії.

Не всі системи контролю доступу працюють за однією схемою. На сьогоднішній день існує чотири типи систем контролю доступу. Кожен тип має свої переваги та недоліки, тому система СКУД обирається індивідуально під конкретні унікальні потреби компанії.

Дискреційний контроль доступу. Головною особливістю даної системи є можливість власнику надати доступ окремій групі людей до окремих місць . Кожна точка доступу містить список дозволених працівників. Така система працює з використанням карти доступу, якщо вона викрадається, то дані блокують, і є можливість встановити пін-код або біометричні дані. Тут налаштування доступів встановлюється автоматично. Системи DAC є найбільш гнучкими, та варіантів доступу існує значно більше в порівнянні з іншими системами.

Обов'язковий контроль доступу. Обов’язковий контроль доступу є найбільш безпечною системою контролю доступу. Доступ є лише в зберігачів та власників. Усі доступи та налаштування встановлюються лише адміністратором, та не можуть бути змінені або вилучені без його дозволу. Система працює за допомогою класифікації усіх користувачів та надає їм доступ відповідно до її програми. Обов’язковий контроль доступу - це суворий та безпечний вид контролю. Недоліком системи - є гнучкість. Такий тип контролю використовується частіше в банках, державних службах, тощо.

Контроль доступу на основі ролей. За останні роки даний тип доступу стає все популярнішим. Він славиться забезпеченням доступу для окремої посади. Це сильно скорочує час для налаштування доступу користувачів.

Контроль доступу на основі правил. **У**правління доступом на основі правил змінює дозволи, базуючись на наборі правил, які були створені адміністратором. Коли суб’єкт бажає отримати доступ до конкретного об’єкта, то йому треба додержуватися набору попередніх правил. Вони можуть бути простими та прямолінійними, а також існує набір правил (складні).

1.1.4 Основні компоненти контролю доступу

Контроль доступу - це запобіжний захід, який вводиться для контролю осіб, які можуть мати доступ до обмеженого простору. Різні приклади контролю доступу можна побачити в системах захисту дверей, замках з ключами, огорожах, біометричних системах, детекторах руху, системі бейджів і т. ін. Створення або проектування дієвих заходів безпеки за допомогою систем контролю доступу починається з розуміння основних компонентів контролю доступу. Він складається з таких елементів:

- ідентифікація суб'єкта доступу полягає в тому, що суб'єкт повідомляє системі ідентифікаційну інформацію про себе (ім'я, обліковий номер і т.д.) і таким чином ідентифікує себе;
- автентифікація (authentication) запобігає доступ до мережі "лівих" осіб і дозволяє вхід для зареєстрованих користувачів. Порядок автентифікації слід відрізняти від порядку ідентифікації. Авторизація суб'єкта доступу відбувається після успішної ідентифікації і автентифікації. При авторизації суб'єкта операційна система виконує дії, необхідні для того, щоб суб'єкт міг розпочати роботу в системі. Наприклад, авторизація користувача в операційній системі UNIX включає в себе появу процесу, що є операційною підсистемою, з якої надалі буде взаємодіяти суб'єкт;
- авторизація суб'єкта не відноситься безпосередньо до захисної оболонки операційної системи. В процесі авторизації вирішуються чисто технічні завдання, що пов'язані з організацією в системі вже ідентифікованого та автенфікованого суб'єкта доступу [8].

Важливо те, що системи автентифікації і авторизації спільно виконують одну задачу, тому необхідно надавати той самий рівень вимог, як до систем авторизації, так і до систем автентифікації. Ненадійність однієї ланки тут не може

бути компенсована кращою якістю іншої ланки. У разі використання паролів при автентифікації потрібні надзвичайні заходи з приводу їх захисту. Одного разу викрадений пароль відкриває двері до всіх засобів та інформації, з якими суб'єкт з цим паролем взаємодіяв [9].

Сучасні рішення контролю доступу запровадили змішаний варіант застосування апаратних і програмних компонентів, і вивчення їх функціоналу та мети, дадуть змогу зрозуміти, як вони працюють. До таких компонентів належать облікові дані та програмне забезпечення (ПЗ). Облікові дані - це інформація, яка ідентифікує суб'єкт та надає йому доступ. Вони є найбільш відомою частиною СКД. Брелки, картки доступу та ідентифікаційні значки являють собою традиційні та загальні облікові дані. Вони кращі за звичайні ключі, оскільки у випадку втрати чи крадіжки, блокується доступ у системі, і вони стають непридатними для сторонніх. Останні розробки в сегменті біометрії дають змогу застосування нових типів облікових даних: відбитки пальців, сканування райдужної оболонки очей, розпізнавання осіб та інше. Технології настільки швидко розвиваються, що їх с кожним днем стає дедалі тяжче вразити, і наразі це є один з найнебезпечніших варіантів контролю доступу до персональної інформації.

Програмне забезпечення (ПЗ) має функцію, яка робить сучасні системи контролю доступу вже такими, якими вони існують наразі. ПЗ дає можливість суб'єктам визначати правила, за якими відбуватиметься надання і обмеження доступу спеціальним персонам в залежності від їх ролей чи посад. Для налаштування СКУД не потрібно контактувати з охороною і чекати, поки спеціалісти завершать необхідні налагодження доступу. ПЗ контролює усі деталі системи, коли саме ж у цей час контролюється певним користувачем. Воно дає можливість створювати звіти, які дозволять відстежувати діяльність на підприємстві. Таким чином це дає можливість моніторити не тільки людей, які мають доступ до необхідних інформаційних областей, а й те як цей доступ використовується, та перевірити, чи не піддається він порушенням.

Не дивлячись на вузьку спрямованість, по установці і використання СКУД діляться на кілька видів. Відмінними рисами різних типів є їх автономна здатність, принцип дії і комплектація. Як правило, системи контролю та управління доступом мають наступні складові: перегороджуючий пристрій (електромагнітні замки, двері, турнікети); ідентифікатор (картка, брелок, відбиток пальця); контролер - механізм, який визначає пропускну можливість ідентифікатора; зчитувач - пристрій, який визначає код ідентифікатора і передає його на контролер. ПЗ та будь-яке додаткове устаткування теж входить до складу системи, в залежності від її типу.

1.2 Переваги хмарної системи контролю доступу над серверною

Все більше і більше компаній усвідомлюють переваги впровадження систем контролю доступу. Вони визнають, що контроль за захистом персональних даних має дуже важливе значення.

Після прийняття рішення про необхідність впровадити систему контролю доступу, клієнтові потрібно вибрати, чи хоче він використовувати хмарне сховище або локальне серверне ПЗ. Більшість обговорень призводить до хмарної системи контролю доступу з таких причин:

1. Хмарний контроль доступу ідеально підходить для компаній з великим товарообігом або кількома сайтами. За допомогою хмарної інфраструктури безпеки можна управляти доступом з однієї платформи для кожного працівника. Централізоване управління та моніторинг дозволів на доступ забезпечує високий рівень гнучкості для бізнесу та реальну перевагу над конкурентами. Компанії можуть створювати конкретні бізнес-моделі, адаптовані до використання цільової групи.

2. Більше комфорту. Якщо потрібно передати дані з локальної системи, можна увійти безпосередньо на веб-портал і переглянути відповідні дані за допомогою хмарної системи контролю доступу. Це простіше і зручніше.

3. Доступ з любого місця. На відміну від локальних систем, хмарні системи контролю доступу працюють в режимі реального часу і дозволяють діяти швидше. Особливо для управління користувачам екстранету, це допомагає надавати дозволи віддалено. Таким чином, спеціальні права доступу до сторонніх постачальників значно спрощуються. Це не тільки забезпечує комфорт у використанні, але також дозволяє виявляти порушення в діяльності доступу та, якщо потрібно, вжити швидких заходів.

4. Підвищена безпека. Автоматичні оновлення ПЗ та виправлення важливі для того, щоб забезпечити оновлення системи контролю доступу та усунення будь-яких потенційних слабкостей. За допомогою хмарної системи контролю доступу оновлення проходять швидко та автоматично. Це сприяє підвищенню ефективності та безпеки системи та зменшує ризик людських помилок.

5. Інтеграції. Відкриті інтерфейси дозволяють впроваджувати зовнішні служби у ваші власні охоронні служби. Мета: автоматизовані робочі процеси та економія часу та витрат.

6. Нові програми. Хмарний доступ відкриває абсолютно нові можливості. Підключаючи кілька служб, процеси можна оптимізувати. Завдяки хмарному контролю доступу, для прикладу, постачальникам послуг надається доступ і дозволяється зберігати свої товари без присутності власника.

Традиційні системи контролю доступу були розроблені для забезпечення доступу без ключів та з можливістю централізованого управління безпекою великих комерційних будівель або житлових об'єктів. Це вважається проривом у технології безпеки. Однак у цих систем є деякі недоліки, включаючи високі інвестиційні та IT-витрати, а також обмежену гнучкість мережі щодо кількості дверей, якими можна керувати. Тепер, застосовуючи хмарні системи, більша кількість підприємств може отримати контроль доступу в повній мірі та додатково багато інших розширених функціями.

Компанії все ще можуть моніторити дозволи на в’їзд, передивлятися дані про дорожній рух, забезпечувати тимчасовий доступ працівникам, які працюють за контрактом, а також здійснювати контроль обігу часу співробітників.

Крім того, завдяки запровадженню хмарних обчислень для цього не потрібно мати дорогі сервери і все можна легко запрограмувати відповідно до потреб кожного бізнесу.

1.2.1 Профільна система контролю доступу

Для захисту даних у хмарному середовищі пропонується механізм контролю доступу на основі профілю, котрий базується на концепції списку контролю доступу. Традиційно фільтрація використовується на основі вхідного трафіку та заздалегідь описаних правил. Ідентифікатор правила вказує на словник, де визначено всі CRUD-операції (створення, видалення, оновлення та отримання) для кожного суб'єкта в системі. Після ідентифікація працівника система генерує маркер доступу служби для цього суб'єкта та надає йому необхідний доступ. Даний механізм допомагає мінімізувати запити на автентифікацію та без зайвих запитів надає доступ до необхідних сервісів.

Персоналізація профілю чи користувача не є новою концепцією у світі контролю доступу до персональних даних. В наш час персоналізація широко використовується для персоналізації вмісту, який відповідає заданому профілю. Профіль - це сутність, яка має заздалегідь визначені адміністратором привілеї для доступу. На першому кроці користувач надсилає свої облікові дані на хмарний шлюз, де служба автентифікації перевіряє користувача. Після перевірки служба надання профілів перевіряє інформацію і генерує маркер доступу користувача до конкретної служби. Токен доступу закінчується, коли користувач виходить із приміщення, реєструючи своє місцезнаходження, або коли сеанс доступу закінчується.

1.3. Огляд літературних джерел

Ґрунтовним вивченням проблеми системи контролю до персональних даних займалися наступні вчені: К.І.Бєляков, В.М.Брижко, М.В.Гуцалюк та інші

[10-13]. Однак все одно комплекс проблем все ширшає, що зумовлює актуальність даної роботи.

В навчальному посібнику [14] розглядаються всі компоненти забезпечення безпеки. Автор детально описує кожну складову. Проводить огляд, в тому числі пристроїв ідентифікації, видів виконавчих пристроїв і контролерів СКУД. Дається оцінка впливу СКУД на забезпечення безпеки об'єкта.

В статті Фаткуліна А.Н. [15] представляє короткий аналіз сучасних систем контролю і управління доступом, відображені існуючі проблеми їх експлуатації, розроблено управління доступом, що дозволяє підвищити рівень їх надійності.

В роботах [16-19] розглядається захист персональних даних робітників навчальних, медичних закладах, працівників готелю, що є завданням адміністрації цих закладів. Статті присвячені питанням модернізації систем захисту інформації, питанням захисту персональних даних, а також впровадженням AHD-систем.

Важливою темою є варіанти захисту персональних даних, що є основним питанням статті Грибової В.В. [20], ґрунтуючись на отриманих теоретичних знаннях, був реалізований прототип роботизованого протеза руки і написана програма, що реалізує рух пальців, щоб обмежити доступ небажаних осіб, а все стало більш роботизованим.

Найголовнішою проблемою є неконтрольоване поширення персональних даних, що оглядається та описується в працях [21-27]. Серед загроз в інформаційній безпеці виділяють дві групи: зовнішні та внутрішні [28]. Якщо опинитися за межами інформаційної системи, що є захищеною, то персональні дані можуть стати доступними майже усім людям, які можна використати, завдаючи шкоди їх власнику [29].

Світова статистика показує, що втрата всього 20% інформації може зруйнувати 65% компаній [30], а спотворення її змісту призведе до катастрофічних наслідків, розторгнення договорів, втратою партнерських відносин, які стануть не зовсім ефективними при розголошенні персональної інформації. При

цьому дослідження вказують, що біля 75% збігу інформації відбувається за розголошенням працівників фірм, 25% завжди готові продати комерційну таємницю [31]. Тому важливим внеском буде створення сучасної системи інформаційної безпеки від несанкціонованого доступу. Волков Я. забезпечує, що така система максимально скоротити величину ризиків втрати інформації [32].

Комітет Міністрів Ради Європи зазначає, що права людини в захисті її персональних даних відноситься, як до офлайн режиму, так і до онлайн простору. Ніхто не має права втручатися до особистої інформації під час її перебування в інтернеті [33]. Л. Тарасенко описує, що цифрове середовище набагато більше ніж мережа Інтернет, під цю категорію попадають не лише веб-сторінки, а й електронні документи, файли, тощо [34].

Проблема витоку інформації може бути також не на рівні особи, а на рівні країн [35-37]. Так питанням правового регулювання суспільних відносин між країнами, які пов’язані з електронним підписом, займалися такі вчені, як Пономаренко Л., Янчева Л., Венбо М., Петров А. А головною темою була проблема компрометації в контексті компрометації особистого ключа електронного підпису [38-39].

Аналіз літератури приводить до висновку, що тема “Система контролю доступу до персональних даних” наразі є актуальною.

1.4. Висновки до першого розділу

У цьому розділі були розглянуті загальні принципи роботи системи контролю доступу, проаналізовано її основні можливості. Наведено головні компоненти систем контролю і управління доступом. Підсумовуючи наведену в першому розділі роботи інформацію, можна підсумувати, що система контролю доступу до персональних даних є актуальною задачею, вирішення якого спрямовано на збереження особистих даних людей.

Сьогодні багато підприємств, у прагненнях забезпечити інформаційний захист своєї комерційної діяльності, підкріплюють формальні заходи (такі як

підписання договорів про нерозголошення інформації) практичними заходами безпечного характеру, в рамках яких тим чи іншим чином порушується недоторканність приватного життя працівників. І тут інтереси бізнесу можуть вступати в конфлікт з принципом неприпустимість втручання в особисте життя.

Розглянувши функціональні можливості СКУД, вимоги до них, оцінивши методи ідентифікації можна зробити висновок, що СКУД це система, основне завдання якої управління доступом на задану територію, що включає можливості розмежування прав доступу, що дозволяє проводити ідентифікацію користувача і включає додаткові аналітичні функції. Сукупність різних методів ідентифікації дозволяє організувати максимальний рівень захисту об'єкта від несанкціонованого доступу. Вибір методів повинен ґрунтуватися на рівні секретності приміщення, в яке надається доступ.

Саме тому тема “Система контролю доступу до персональних даних” є актуальною.

РОЗДІЛ 2. ПОРІВНЯННЯ ТА АНАЛІЗ СИСТЕМ КОНТРОЛЮ УПРАВЛІННЯ ДОСТУПОМ

2.1. Система контролю управління доступом

Система контролю і управління доступом, СКУД (англ. Access Control System, ACS) - сукупність програмних і апаратних засобів, які забезпечують захист об'єкта від несанкціонованого проникнення. Система контролю і управління доступом відіграє важливу роль в комплексній системі охорони підприємства, забезпечує збереження майна споруд і працівників.

Розрізняють централізовані та автономні системи СКУД.

Централізовані системи, це системи де контролери з’єднано в єдиній мережі та приєднано до ПК, що керує всією системою. До комплексу наявних систем входять: відеоспостереження, пожежна та охоронна сигналізації. Їх використовують на великих промислових зонах де працює багато працівників та відвідувачів. Ця система дозволить одночасного управляти значною кількістю пунктів пропусків, робити зміни в програмі та додавати нову функціональність.

Автономні — самостійно керують роботою периферійних елементів та контролюють точки доступу. Використовуються в суспільних, адміністративних закладах та закладах освіти, приватних будинках тощо.

СКУД – це ефективні рішення, які здатні заборонити вхід в приміщення стороннім людям, дозволяють контролювати вхід особам які можуть це зробити, і отримати при цьому усю необхідну статистику та забороняти вхід особам яким це заборонено. Системи моніторингу доступу дають можливість дізнатися, хто, в який час і скільки людей прийшло через пункт пропуску, наскільки часто вони ходять на перекур, коли покидають робочу зону. Вся одержана статистика таблицею списком і так далі, дивлячись яке ПЗ було встановлено і як

настроєно). Головне завдання такої системи – контроль допуску на об’єкт людей. Загальна структура СКУД зображена на рис. 2.1.

Рис. 2.1. Архітектура СКУД

Принцип функціонування системи контролю та управління доступом можна проаналізувати на наступному прикладі: Кожен працівник, клієнт або відвідувач отримує ід, ідентифікатор (електронний ключ) - пластмасову карточку або брилок на якій розміщений код. "Електронні ключі" даються в результаті проходження реєстрації співробітників за допомогою системного обладнання. Паспортні дані, (відео, фото) та інші дані про господаря "електронного ключа" вносяться в особисту "електронну карточку". Особиста "електронна карточка" власника та його код "електронного ключа" з’єднуються один з одним і вносяться в комп'ютерні бази даних.

На вході в будинок або всередині приміщення встановлюються карткові зчитувачі, що читають інформацію з карток та їх код, дані про права доступу власника карточки і відправляють інформацію до контролера цієї системи. В системі для кожного коду є відповідність код-інформація про права власника карточки. При порівнянні інформації, при якій була пред'явлена карточка, сис-

тема приймає рішення: контролер дає доступ або блокує його (двері, замки, турнікети), переводить будівлю в спеціальний режим охорони, або за потреби вмикає сигнал тривоги.

2.2. Огляд існуючих систем контролю доступу до персональних даних

Зазвичай система контролю і управління доступом складається з різних компонентів, починаючи з тих, які роблять ідентифікацію працівника, і закінчуючи тими, що вирішують чи надавати доступ.

Якщо вам потрібно інсталювати СКУД, то вам потрібні будуть наступні компоненти:

- ідентифікація осіб, які мають право доступу;
- розмежування доступу до різних приміщень;
- керування автоматичними режимами;
- реєстрація часу перебування особи на об’єкті;
- обробка інформації та ведення статистики.

Системи захисту та контролю доступу до даних бувають як апаратні так і програмні.

До апаратних систем належать:

- ідентифікатори;
- зчитувачі;
- виконавчі пристрої;
- електрозамки;
- турнікети;
- контролери;
- автономні контролери СКУД;
- мережеві контролери СКУД.

Програмні засоби захисту даних та контролю доступу до них відрізняються від апаратних тим що їх не можливо пощупати руками вони існують тільки у віртуальному середовищі.

Найчастіше програмні засоби захисту інформації використовують для виконання наступних процесів: ідентифікація й автентифікація користувача, розмежування та доступ користувача до інформаційної мережі, пін захист і перевірка прав доступу, шифрування інформації, а також захист від несанкціонованих змін, зчитування чи копіювання.

Найпоширенішими прикладами програмних засобів захисту інформації є такі:

- система контролю і управління доступом;
- антивірусні програми;
- шифрувальне програмне забезпечення;
- мережевий екран;
- система виявлення вторгнень;
- керування записами[en];
- пісочниця;
- система управління інформаційною безпекою
- SIEM.

2.3 Шифрування даних

Двадцять перше століття - століття інформатики та автоматизації. Технології дозволяють відсилати і зберігати великі об'єми особистої інформації. Це також має й протилежний бік. Більш уразливою стає інформація:

- обсяги інформації ростуть;
- збільшується частка користувачів, які мають доступ до ресурсів електронних обчислювальних машин, програм та даних;
- ускладняються можливості застосування ЕОМ.

Тому проблема забезпечення інформації від несанкціонованого доступу (НСД) стає дедалі важливішою проблемою при передачі і зберіганні даних. Захист інформації - сукупність методів, заходів і засобів, що запобігають обмеженню несанкціонованого доступу до ресурсів ЕОМ та інформації; забезпечують перевірку цілісності даних; здійснюють усунення несанкціонованого застосування програм (захист програм від копіювання).

Метод шифрування (криптографія) - є основою захисту інформації від несанкціонованого доступу, що частіше використовується при контролюванні доступу до персональних даних. За участі спеціальних ключових правил, шифрування перетворює відкриті дані в зашифровані або ж навпаки (див. рис. 2.2). Можливості криптографічних методів:

- шифрування інформації;
- розподіл ключів шифрування;
- реалізація ЕЦП (електронного підпису);
- захист від навмисної зміни інформації.

Шифрувальні алгоритми мають певні вимоги: високий рівень забезпечення персональних даних від дешифрування і модифікації; захищеність інформації прив'язана тільки до знання ключа і не залежить від того, часто використовуваний алгоритм чи ні; мала зміна вихідного тексту або ключа повинна приводити до значної зміни шифрованого тексту (так званий ефект "обвалу"); діапазон значень ключів повинен прибирати можливість дешифрування інформації шляхом знаходження значень ключів; економічність реалізації алгоритму при достатній швидкодії; вартість дешифрування даних без знання ключа повинна перевищувати вартість самих даних.

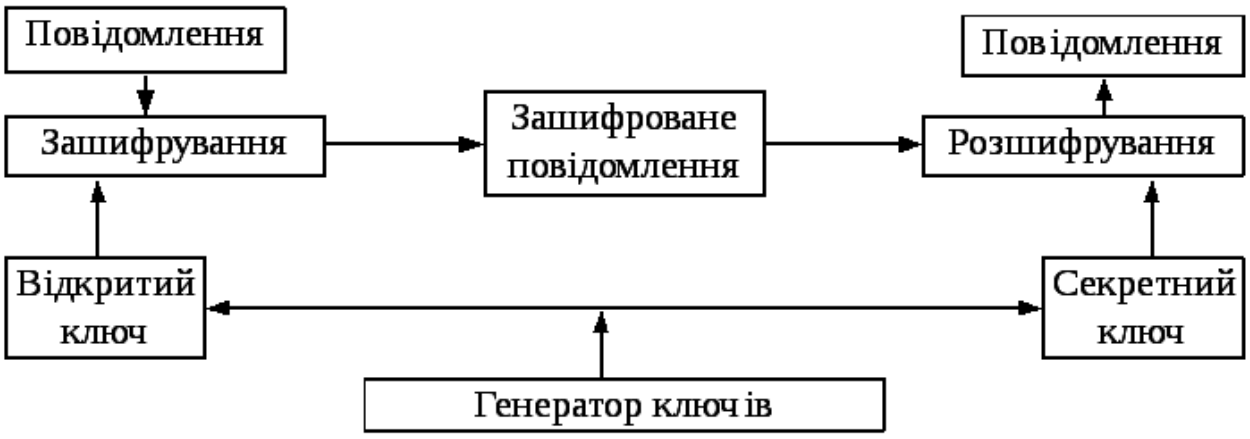

Рис. 2.2. Схема роботи шифрування даних

Спільне застосування різних видів шифрування як для передачі інформації, так і її зберігання на диску дасть найбільший рівень захисту, ніж використання якогось одного з цих видів шифрування. Спеціалісти називають такий спосіб «глибоким захистом». Застосовуючи кілька способів захисту даних, ви можете досягти максимального рівня безпеки. До прикладу, якщо ви надсилаєте незашифровані повідомлення (НЕ шифруєте передачу даних) з зашифрованого мобільного пристрою (яке шифрує всі дані, що зберігаються), ці повідомлення будуть уразливі для перехвату з боку урядів, постачальників послуг або технічно підкованих зловмисників. А повідомлення, записані на мобільному пристрої, навпаки будуть захищені від зловмисників, що мають фізичний доступ до пристрою, але не знають пароля.

2.4. Авторизація за допомогою SSH протоколу

SSH (від англ. "Secure Shell") - це протокол віддаленого адміністрування, створений для здійснення віддаленого управління операційними системами і тунелювання TCP-з'єднання. Застосування цього протоколу допускає використання різних алгоритмів шифрування, що дає змогу безпечно працювати практично в будь-якому незахищеному середовищі: працювати з ПК через командну систему, відсилати по зашифрованому каналу будь-який тип інформації (на-

приклад, відео- та аудіофайли). Перший реліз протоколу відбувся в 1995 р, а вже в 1996 р була представлена покращена його версія, яка і стала основою для розвитку продукту. Сьогодні для всіх мережевих ОС доступні SSH сервер і SSH клієнт, а сам протокол SSH є одним з найбільш популярних рішень для віддаленого управління системами і передачі важливої інформації [4].

SSH - це комерційний продукт і надається на платній основі. Існує і не комерційна версія - OpenSSH, більшість програмістів використовують саме її. Деякі навіть вважають, що в силу свого відкритого вихідного коду, вона більш захищена і зручна у використанні.

Застосування SSH підключення має ряд переваг: забезпечена робота на віддаленому ПК із використанням командної оболонки та різних алгоритмів шифрування (симетричного і асиметричного хешування); можливість безпечного використання будь-якого мережевого протоколу, що забезпечує захищений обмін файлами будь-якого розміру.

2.5. Двофакторна автентифікація

Протягом останніх років практично всі популярні поштові служби, сервіси електронних платежів, банки ввели багатоетапну (або багатофакторну) автентифікація для своїх клієнтів. Такі заходи дозволяють ефективніше захистити персональні дані від крадіжки (див. рис. 2.3).

Багатофакторною автентифікацією називають автентифікацію, при якій використовуються автентифікаційні ознаки різних типів (зауважимо, не кілька ознак, а ознаки декількох типів) [5]. Типи автентифікаційних ознак і називаються автентифікаційними факторами.

Двофакторна автентифікація - це додатковий рівень захисту облікового запису. Крім введення пароля, потрібно також ввести одноразовий код, який приходить на пошту або телефон, або відбиток пальця. Цим підтверджується своя особистість. Коли активується дана опція, крім пароля хакеру потрібно також ввести код, щоб зайти в потрібний аккаунт. Та людина, сторінку якої нама-

гаються зламати, також отримає повідомлення, що хтось намагається отримати доступ до сторінки. Одноразовий код діє лише пару хвилин або годин, після чого він самознищується. Таким чином, завдяки двофакторній автентифікації онлайн-аккаунти стають невразливими для кіберзлочинців.

Бажано застосовувати багатофакторну автентифікацію на будь-яких сайтах, що зберігають особисті дані (соцмережі, електронна пошта, інтернет-банк і т.д.), навіть якщо сервіс дозволяє обійтися без неї. Звичайно, це не завжди комфортно, але практично завжди робить відвідування важливих сайтів більш безпечним.

Рис. 2.3 Схема роботи двофакторної автентифікації

2.6. Авторизація через USB-ключ доступу

Токен авторизації або USB-ключ - це пристрій (носій) невеликого розміру, який допомагає забезпечити інформаційну безпеку володарям, також використовується для підтвердження його власника, застосовується для віддаленого доступу до різних інформаційних ресурсів. Простою мовою “токен” - це електронний ключ для доступу до чого-небудь.

Токен авторизації зовні схожий на USB-накопичувач (флешку), але він має карту пам'яті, яка захищена паролем, на ній знаходиться інформація для ге-

нерації електронного цифрового підпису (ЕЦП). Щоб ідентифікувати себе, господар ЕЦП повинен вставити токен в USB-вхід на комп'ютері і ввести пароль.

Токен дозволяє забезпечити надійний захист закритих ключів ЕЦП в спеціальній області пам'яті, з якої ці ключі ніяк не витягнути без знання пароля. При цьому один ключ токен дозволяє зберігати закриті ключі декількох ЕЦП, що дає можливість відповідальним особам підписувати електронні документи різними ЕЦП (наприклад, для різних організацій). використання в системах віддаленого банківського обслуговування - токен застосовують для входу і здійснення банківських операцій онлайн на сайті банку; можливість участі в електронних торгах; місце зберігання цифрових сертифікатів для роботи в системі електронних державних послуг; підвищення безпеки роботи в електронній пошті; захист електронного документообігу.

Смарт-карти і USB брелки призначені для захисту даних, шифрування і автентифікації у великих мережах. Їх установкою і запровадженням має керувати фахівець. Щоб зрозуміти, чому такий собі звичайний USB накопичувач є кращим вибором для захисту персонального комп'ютера або малого офісу, розглянемо особливості смарт-карт і USB брелків. Смарт-карта - це пластикова картка з вбудованим мікрочіпом (мікропроцесор і пам'ять), на зразок банківської або телефонної картки. Для роботи зі смарт-картами потрібно спеціальний пристрій - смарт-карт зчитувач. Для нього потрібно інсталювати спеціальні драйвера. Смарт-карту необхідно підготувати (відформатувати/персоналізувати) перед першим застосуванням за допомогою спеціальної програми. Розмір пам'яті смарт-карти надзвичайно малий (кілька кілобайт), оскільки пам'ять в смарт-картах призначена тільки для зберігання малих обсягів інформації (цифрових сертифікатів, ключів шифрування, паролів). І вам необхідно переконатися, що розмір пам'яті підійде для ваших цілей. А якщо раптом пам'ять на карті закінчиться? Оскільки деяким працівникам необхідно мати доступ до кількох систем, то їх смарт-карти повинні містити більше інформації. Програми, які працюють зі смарт-картами зазвичай підтримують саме ваш тип

смарт-карт (або кілька). Але не все відразу. Необхідно переконатися що для смарт-карт, які у вас є в розпорядженні, можна знайти ПЗ для ваших потреб.

Єдиним мінусом токенов є їх вразливість, їх легко втратити або викрасти, але ситуацію знову рятують паролі, без яких не електронні цифрові підписи нічого не варті.

2.7 Захист даних на рівні бази даних, програмний захист даних

Дані — це найцінніший корпоративний актив для будь-якого бізнесу. Незалежно від того, в якій галузі працює підприємство, важливо дбати про фінансові звіти, медичні записи або бізнес-плани для підприємства. База даних (БД) — це структурована сукупність інформації, яку можна зберігати, аналізувати та обробляти за допомогою СУБД (системи управління базами даних). Бази даних необхідно захищати та регулярно перевіряти актуальність цього захисту. Використовуючи спеціальні програми та методики, можна запобігти несанкціонованому доступу (НСД) до бази даних в локальних мережах або витоку інформації, не призначеної для широкого розголосу.

2.7.1 Нормалізація бази даних

Нормалізація відношень – покроковий процес розділення (декомпозиції) початкових відношень БД на простіші. Кроки нормалізації переносять схему БД зодного виду в інший що дозволяє, більш правильно її використовувати і уникнути проблем в майбутньому. Кожна наступна форма володіє кращими властивостями ніж попередня. Кожній нормальній формі відповідає певний набір обмежень. При переведенні структури відношення у з форми нищого порядку до форми вищого порядку досягають оптимізації інформації. Процес нормалізації оснований на функціональній залежності атрибутів.

Перша нормальна форма . Відношення відповідає 1NF тоді, коли на перетині кожного стовпця і кожного рядка знаходиться тільки елементарна (неподільна) одиниця, атрибут і не містяться групи елементів, що повторюються (див. рис. 2.4).

Друга нормальна форма. Відношення знаходиться в 2NF, якщо виконується обмеження 1NF і кожен атрибут функціонально залежить від первинного ключа.

Рис. 2.4. Перша нормальна форма

Третя нормальна форма. Відношення знаходиться у 3NF, якщо знаходиться у 2NF і всі атрибути відношення взаємно незалежні і повністю в залежності від первинного ключа, тобто кожен атрибут не транзитивно залежить від ключа.

Четверта нормальна форма (4НФ, 4NF) вимагає, аби в схемі баз даних не було нетривіальних багатозначних залежностей множин атрибутів від будь чого, окрім надмножини ключа-кандидата. Таблиця знаходиться у 4НФ тоді, і тільки тоді, коли вона знаходиться в НФБК, та її багатозначні залежності є фу-

нкціональними залежностями. Завдяки четвертої нормальної форми можна позбутись небажаних структур даних — та багатозначних залежностей.

П'ята нормальна форма (5НФ, 5NF, PJ/NF) вимагає, аби не було не тривіальних залежностей, які б не виходили із обмежень ключів. Таблиця в п'ятій нормальній формі, тоді, коли вона знаходиться в 4НФ, та кожна залежність об'єднання обумовлена її ключами-кандидатами.

Шоста нормальна форма. Таблиця знаходиться у 6nf, якщо вона знаходиться у 5НФ та задовольняє вимогам відсутності нетривіальних залежностей. Зазвичай 6nf тотожна з dknf.

Цілі нормалізаці: позбутись подвоєння інформації в таблицях. Надати можливість змін у структурі нормалізованих таблиць. Зменшити вплив структурних змін бази даних на роботу додатків, які забезпечують користувачам доступ до даних.

2.7.2 Захист інформації в базах даних

У сучасних СУБД надається один з двох підходів до питання забезпечення безпеки даних: виборчий підхід і також обов'язковий підхід. В тому і в тому підході одиницею даних, для яких має бути створена система безпеки, може бути як вся база даних цілком, так і будь-який об'єкт всередині бази даних. Отже ці два підходи вирізняються такими властивостями: Коли є виборчк управління користувач має різні права (привілеї чи повноваження) у роботі з такими об'єктами. Різні користувачі можуть володіти різними правами доступу до того ж самого об'єкту.

Виборчі права володіють значною гнучкістю. У разі виборчого управління, кожен об'єкт даних присвоює собі класифікаційний рівень, а кожний користувач системи має певний рівень допуску. За цим підходом доступ до певного об'єкту даних є тільки в користувачів з певним рівнем допуску до системи.

Щоб реалізувати певний виборчий принцип передбачають наступні методи. У базу даних заповнюється новий тип об'єкту БД - користувач. Кожному

юзерові в Базі Даних ставиться у відповідність ідентифікатор. Для більшого захисту кожному користувачеві окрім унікального ідентифікатора надається унікальний пароль, до того ж якщо ідентифікатори юзерів доступні системному адміністраторові, то паролі юзерів зберігатимуться найчастіше в кодовому вигляді і доступні лише самому користувачеві. Юзери можуть бути об'єднані в спеціальні групи користувачів.

Користувач може входити не тільки в одну групу, а й у кілька груп. У стандартному вигляді вводяться поняття групи PUBLIC, для якої має бути мінімальний набір прав. За замовчуванням кожен новий юзер належить до групи PUBLIC. Привілеї чи спеціальні повноваження користувачів або груп - це набір операцій, які вони можуть виконати над об'єктом БД. В останніх сценаріях переліку СУБД з'явилися нове значення "ролі".

Роль - це іменований набір повноважень користувача. Існує ряд спеціальних ролей, які визначаються в момент з’єднання сервера баз даних. Також є можливість створити нові ролі, групуючи їх з різними повноваженнями. Застосування ролей забезпечує спрощення управління привілеями юзерів, та структурувати цей процес. Окрім цього, введення ролі не зв'язане з конкретними користувачами, отже роль може бути визначена і сконфігурована до того, як визначаються користувачі системи. Користувачеві може зазвичай призначається одна або кілька ролей.

Об'єктами Бази Даних, які мають бути захищені, є всі дані, що знаходяться в БД: таблиці, збережені процедури, подання і тригери. У конкретного типу об'єкта є свої власні дії, тому для кожного з об'єктів можуть бути визначені різні права доступу. На найпростішому рівні концепції безпека бази даних майже не забезпечується. Потрібно забезпечити два основних принципи: перевірення повноважень і перевірку автентичності (автентифікацію). Перевірка правд доступу і того що може зробити користувач забезпечується на тому, що кожному юзерові або процесу інфо-системи є відповідність набору дій, що він може виконувати по відношенню до конкретних об'єктів.

Перевірка автентичності визначає підтвердження того, що користувач або процес, який намагається виконати дозволену дію, дійсно той, ким він є насправді.

Система призначення повноважень має в деякому роді ієрархічний характер. Найвищі права доступу має системний адміністратор або адміністратор сервера БД. Отож лише цей тип юзерів може створити інших користувачів і наділити їх певними своєрідними правами.

Кожен об'єкт в БД має свого власника - користувача, що створив цей об'єкт. Власник об'єкта має всі права-повноваженнями на даний об'єкт, у тому числі він має право надавати іншим користувачам повноваження по роботі з даним об'єктом або забирати у користувачів раніше надані повноваження.

SQL-ін’єкція це найнебезпечніший вид атак, тому що завдяки ньому було дуже багато випадків злому різних систем як сайтів так і баз даних і він також є найпростішим способом зламати якусь систему (див. рис. 2.5). Насправді захиститися від цього типу атак досить просто, але нажаль не всі це роблять. Щоб захистити себе від цієї атаки достатньо внести в свій код деякі зміни.

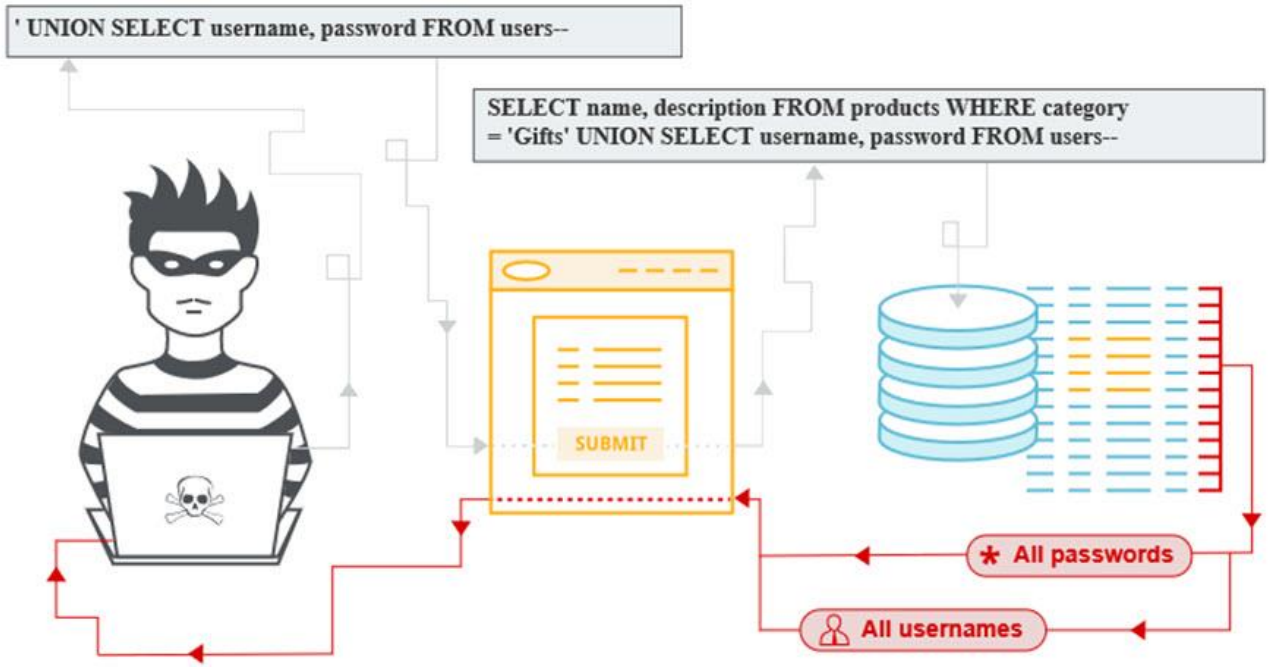

Рис. 2.5 SQL ін’єкції

SQL- ін’єкцією називають дії, які виконує зловмисна сторона, для того щоб виконати свій запит до бази даних, та отримати вашу інформацію без вашого на це дозволу. Найчастіше це відбувається якщо ви відправляєте певну інформацію на сервер, але замість відсилання того запиту який відправляє сайт зловмисник відсилає свій запит, який виконується сервером і видає йому всю необхідну інформацію. За допомогою такого запиту зловмисник може отримати заборонену інформацію з бази даних, а також, внести до неї зміни, і навіть почистити всю базу даних

PHP-ін'єкція — це також один із способів взлому веб-сайтів, що працюють на мові програмування PHP, який полягає у виконанні стороннього коду на серверній стороні веб сайту.

Потенційно небезпечними функціями є:

eval(),
preg_replace() (з модифікатором «e»),
require_once(),
include_once(),
include(),
require(),
create_function().

PHP-ін'єкція стає можливою, якщо вхідні параметри приймаються і використовуються без перевірки.

Для захисту від SQL- та PHP-ін'єкцій використовується спеціальний алгоритм, який забезпечує хешування SHA-256 з сімейства хеш-функцій SHA-2. SHA-2 — збірна назва односторонніх хеш-функцій SHA-224, SHA-256, SHA-384 і SHA-512. Ці хеш-функції призначені для виробництва «відбитків» або «дайджестів» повідомлень будь-якої бітової довжини. Застосовуються в різних додатках або компонентах, пов'язаних із захистом інформації.

Для захисту паролю користувача від зловмисних дій було використано функцію password_hash(). Функція password_hash () використовуються для створення складеного хешу, генерування складної сутності та застосовує пра-

вильно кількість раундів хешування автоматично. Функція password_hash () є обгорткою над crypt () і сумісна з існуючими хешами паролів. Тому для того щоб захистити свою систему від взломів для захисту паролів зазвичай ввикористовують цю функцію.

Деякі операційні системи підтримують кілька алгоритмів хешування. Деколи стандартні алгоритми, засновані на DES, замінюються алгоритмами на основі MD5. Вид хешування забезпечується аргументом salt. До версії PHP 5.3, PHP визначав алгоритми шифрування зразу після інсталяції, базуючись на системній функції crypt ().

Якщо аргумент заглушки salt не вказаний, буде автоматично згенеровано стандартна випадкова двосимвольна (DES) або дванадцятисимвольний (MD5) аргумент, в залежності від доступності алгоритму MD5 в crypt ().

Зумовлена константа CRYPT_SALT_LENGTH дозволяє визначити максимально доступну довжину аргументу відповідно до використовуваних алгоритмів.

Дані в системах баз даних мають зберігатися з гарантуванням конфіденційності та безпеки.

Інформація має бути захищена від викрадення. Під безпекою даних у базі розуміють захист даних від випадкового або спланованого доступу до них осіб, які не мають на це права, від несанкціонованого розкриття, зміни або видалення.

Безпека даних підтримується комплексом заходів і засобів:

- організаційно-методичні заходи передбачають розроблення інструкцій та правил, які регламентують доступ до даних та їхнє використання, а також створення відповідних служб і підрозділів, які стежать за дотриманням цих правил;
- правові та юридичні заходи передбачають юридичне закріплення прав і обов'язків щодо зберігання, використання й передавання в електронному вигляді даних, які підлягають захисту, на рівні державних законів та інших нормативних документів;

- Організаційно-технічні засоби захисту - це комплекс технічних засобів, які сприяють вирішенню проблеми захисту даних;
- Програмні засоби захисту це комплекс математичних, алгоритмічних і програмних засобів, шо сприяють вирішенню проблеми захисту даних.

2.7.3 Валідація даних

Валідація (перевірка вхідних даних за певним правилом) — процес, що дозволяє визначити, наскільки точно з позицій потенційного користувача деяка модель представляє задані сутності реального світу.

Неможливо відновити дані після збою. Не завжди програма здатна «повернути все назад». Можливо, в процесі роботи програма виконала якісь незворотні дії - видалила файл, відправила дані по мережі, надрукувала щось на принтер, запустила різець верстата і він частково справив обробку заготовки деталі. Але навіть якщо відновлення в принципі можливо, алгоритм відновлення може теж містити помилки, і це іноді призводить до зовсім сумних наслідків.

Для валідації потрібен доступ до недоступної частини стану системи. Це особливо характерно для перевірки даних, що вводяться людиною через графічний інтерфейс користувача.

Сучасні програми часто побудовані з використанням багаторівневої архітектури, яка передбачає, що реалізація призначеного для користувача інтерфейсу виділена в презентаційний шар, а для перевірки потрібен доступ до інших верств, аж до шару бази даних. Тому в даному проекті проводимо валідацію в тих місцях де можливі помилки при введенні користувачем власної інформації та подальшого її занесення в базу.

Валідацію даних доцільно проводити при реєстрації, авторизації та формах введення даних користувачем. Нижче наведено методи та їх описи, в яких проведена валідація даних.

Відсутність валідації може призводити до вищеописаних (а може бути і ще якимось іншим) проблем. Відповідно, наявність валідації дозволяє запобігти серйозним збоям, спрощує ідентифікацію проблем, але за це доводиться розплачуватися продуктивністю, оскільки додаткові перевірки збільшують навантаження на систему.

2.8 Виявлення проблемних місць системи безпеки підприємства

Практично неможливо мати чітке уявлення про те, наскільки добре виконуються функції системи кібербезпеки, без попереднього аналізу всіх інформаційних активів компанії та виявлення файлів, потенційно становлять інтерес для зловмисників. Якщо компанія нехтує сортуванням своїх даних, вона робить неправильний вибір.

Наприклад, одна фінансова організація почала впроваджувати програму цифровий (digital) стійкості, оцінивши тільки нормативні вимоги. Два роки по тому вони домоглися невеликого технічного прогресу, але було витрачено багато зайвих грошей і всі зусилля на захист персональних даних своїх клієнтів та інших важливих інформаційних активів.

Компанії повинні оцінювати ризики інтегрованим способом. Зловмисник запросто може обійти систему захисту, отримавши доступ до управління, приховавши при цьому своє вторгнення. Треба вжити всіх заходів для того, щоб хакер повинен був перемогти систему захисту, що охоплює різні види контролю, а не тільки ідентифікацію користувача за допомогою логіна і пароля.

Якщо системи захисту будуть взаємопов'язані між собою, яку атакують організація зможе виграти час і запобігти витоку даних. На жаль, багато компаній розглядають кожен елемент системи безпеки: виявлення вторгнень, I & AM, захист даних, звіт про інциденти, тощо - окремо. Вони нехтують оцінкою того, як саме перераховані елементи об'єднуються і взаємодіють один з одним для захисту інформації.

Підприємство повинно вийти за рамки традиційного захисту своїх даних. Повсюдно керівники кажуть, що їм хочеться отримати оцінку контролю безпеки. На жаль, їх в основному цікавлять тільки такі тактичні проблеми, як ефективність інструментарію виявлення вторгнень або наявність шкідливих програм. В результаті зазвичай виходить, що будь-яка зміна відбувається в рамках вкрай обмеженої системи безпеки. Для досягнення серйозних результатів, компанії часто мають самостійно здійснювати всі бізнес-процеси, змінюючи їх в контексті більш широких стратегічних і оперативних міркувань.

Ефективна система кібербезпеки - це не тільки адреси існуючих протоколів, персоналізація та інший інструментарій, а ще й управління, контроль, архітектура сервісу і система обміну даними.

План кібербезпеки повинен бути амбіційним, але досяжним і досить простим для пояснення, таким, щоб керівники надавали організаційну підтримку при впровадженні системи і при її використанні.

Після того, як компанія визначить пріоритетні бізнес-ризики, вона зможе використовувати три типи механізмів для підвищення рівня безпеки своїх інформаційних активів:

• елементи керування бізнес-процесами (зміни поведінки користувачів і бізнес-процесів за межами IT);

• ширші можливості управління IT (зміни в архітектурі IT в цілому);

• засоби управління системою кібербезпеки (дискретні технологічні зміни, призначені для захисту інформації, такі як шифрування, I & AM і аналітика безпеки).

Багато компаній занадто багато уваги приділяють засобам контролю за кібербезпекою і тим самим створюють невиправдано дорогі і нав'язливі системи. В ідеалі, вони повинні спиратися на всі три види контролю. Дії повинні бути пріоритетними за кількістю і характером бізнес-ризиків, які вони зачіпають, і по мірі, в якій вони вимагають від організації тих чи інших змін.

Будь-який план повинен включати в себе широкий набір поліпшень, ініціатив та дій, які можна включити в короткий перелік основних стратегічних моментів.

Обов'язковим елементом системи кіберзахисту інформаційного периметра організації повинен бути аудит ІБ. Аудит буває зовнішнім (проводить незалежний підрядник, як правило, разово) і внутрішнім (здійснюється співробітниками ІБ компанії на постійній основі). В ідеалі обидва види аудиту повинні поєднуватися і робитися регулярно. Цілі аудиту:

• дослідити і оцінити рівень захищеності інформаційних систем компанії на поточний момент;

• визначити уразливості, "вузькі місця", схильні до ризику ресурси, потенційні кіберзагрози;

• оцінити потенційні збитки, якщо кіберзагрози будуть реалізовані, і вартість наслідків кібератак;

• виділити пріоритети впровадження заходів щодо захисту систем та захисту інформації;

• мінімізувати ризики і оцінити рентабельність заходів кібербезпеки.

2.9. Визначення способу впровадження системи кібербезпеки

Як тільки компанія визначила свої цілі в області кібербезпеки, втілення намірів у життя вимагає цілого ряду операційних процесів, таких як оновлення прав доступу до облікових записів, оцінка можливостей системи безпеки постачальників, огляд архітектури безпеки додатків.

Історично так склалося, що керівники та IT-фахівці розглядають перераховані засоби контролю, як гальмо для здатності організації досягати бізнес-результатів. І, чесно кажучи, багато аспектів кіберзахисту дійсно діють як обмеження.

Наприклад, нові заходи безпеки для захисту важливих інформаційних активів зажадають введення в організації більш суворої політики щодо паролів і

розмежування прав доступу до інформації та приміщень. Це може сповільнити існуючі процеси, зробити бізнес менш гнучким, розчарувати співробітників і підірвати довіру клієнтів.

Кібербезпека є такий же бізнес-проблемою, як і будь-яка технологічна, і усвідомлення цього нюансу допомагає компанії швидко впроваджувати необхідні зміни з мінімальними витратами.

2.10 Комплексний підхід до реалізації системи інформаційної безпеки

Підсумовуючи вищесказане, комплексний підхід до реалізації ІБ полягає в тому, що захист необхідно здійснювати на трьох ключових рівнях - персоналу, процесів і технологій:

• персонал компанії: користувачі повинні знати і чітко дотримуватися основних принципів інформаційної безпеки: вибір надійних паролів, уважне ставлення до вкладень в електронних листах, резервне копіювання даних, розумне використання зовнішніх інтернет-ресурсів з робочих пристроїв і ін.

• бізнес-процеси і нормативна регламентація: необхідно розробити базовий набір заходів з протидії вживаються і успішно здійсненим атакам. У ньому має пояснюватися, як визначати атаки, захищати системи, виявляти загрози та протидіяти їм, а також відновлювати працездатність робочих систем після здійснених атак.

• технології: ключова ланка в системі ІБ. Основні компоненти, які повинні бути захищені, - так звані кінцеві пристрої: комп'ютери, інтелектуальні пристрої та маршрутизатори, мережі і хмарна середу. Найбільш поширені технології для захисту обладнання - брандмауери, фільтрація DNS, антивірусне ПЗ, рішення для захисту електронної пошти.

2.11. Висновки до другого розділу

У цьому розділі було розглянуто СКУД, проаналізовано її основні види як апаратні так і програмні. Визначено що до апаратних систем належать: ідентифікатори, зчитувачі, виконавчі пристрої, електрозамки, турнікети, контролери, автономні контролери СКУД, мережеві контролери СКУД. Найпоширенішими ж прикладами програмних засобів захисту інформації є: система контролю і управління доступом, антивірусні програми, шифрувальне програмне забезпечення, мережевий екран, система виявлення вторгнень, керування записами, пісочниця, система управління інформаційною безпекою, та SIEM.

Було розглянуто методи та засоби шифрування даних, те як можна авторизуватись за допомогою SSH протоколу, захистити персональні дані за допомогою двофакторної автентифікації та як можна авторизуватись через фізичний USB-ключ носій.

Також було проаналізовано методи нормалізації бази даних та як з їх допомогою можна оптимізувати базу даних, і захистити її скориставшись ефектом нормалізації. Розглянуто способи захисту від найпоширеніших атак на веб сервіси SQL та PHP ін’єкцій, за допомогою програмних засобів, які дозволяють за допомогою спеціальних функцій захистити свій веб-сервіс. Та оглянуто способи валідації даних та те як можна захистититись від введення не правомірних даних.

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1 Розробка системи контролю доступу web-сайту компанії

Будь-який веб-сайт являє собою досить складний і сукупний з модулів продукт, що розробляється, як правило, одночасно декількома фахівцями.

Розробка веб-сайту, процес досить складний і припускає застосування великої сукупності технологій.

Етапи розробки веб-сайту:

- збір технічних вимог і складання технічного завдання;
- створення прототипу веб-сторінки;
- розробка дизайну;
- верстка;
- програмна частина;
- тестування та запуск проекту в production.

Розробка будь-якого веб-сайту, починається зі збору вимог до майбутньому ресурсу, визначення формату ресурсу і цільової аудиторії, але особливо важливу роль буде грати система контролю доступу до інформації.

Саме на цьому етапі задаються перші і фундаментальні завдання майбутнього проекту.

3.2 Створення прототипу, дизайну і верстка сайту

Єдиної вимоги до оформлення прототипів і ПО для їх розробки на сьогоднішній день не існує. На основі прототипу веб-сторінки будує дизайн, прототип і технічне завдання вже практично в повній мірі ілюструють функціонал майбутнього веб-сайту (див. рис. 3.1).

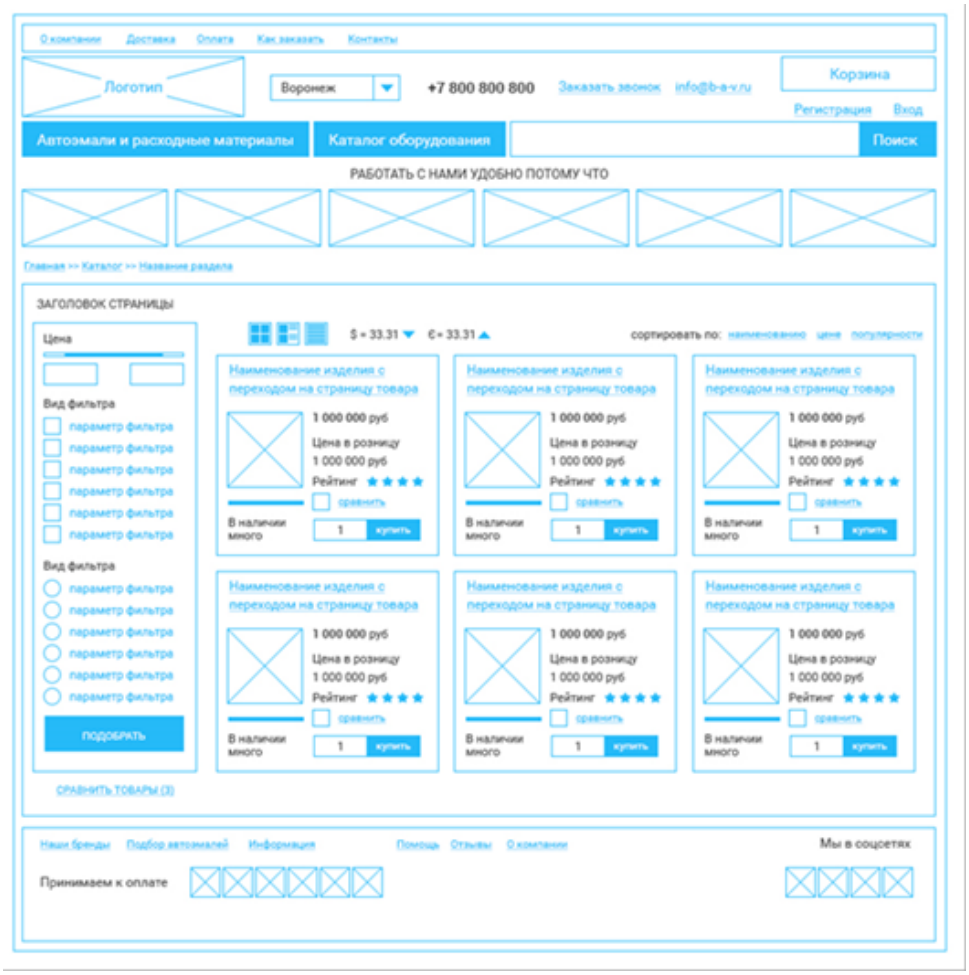

Рис 3.1. Створення прототипу сайту

Прототип сайту повинен враховувати різні рівні доступу і відображати видимі зони, кнопки, сторінки для кожного рівня.

Наприклад, доступ до замовлення товару може отримати тільки зареєстрований користувач, а кнопка входу в панель адміністратора не повинна бути видна користувачам з іншим рівнем доступу.

Далі важливим етапом стає розробка дизайн сторінки, дизайн готується в графічному редакторі. Найбільш популярні графічні редактори для розробки дизайну: Adobe Photoshop, Sketch, Adobe XD, Figma. Останній є онлайн-редактором, строго спрямованим на розробку інтерфейсів.

Після того як готовий дизайн, приступаємо до процесу верстки, створюємо кореневої каталог майбутнього веб-сайту, створюємо головну сторінку і каталоги для вкладення медіа-файлів.

Назви файлів:

• index.php (головна сторінка веб-сайту, за замовчуванням файл з ім'ям index завжди визначає головну сторінку і може бути в інших рас-ширення html, htm і ін.).

• style.css (файл каскадних таблиць стилів, назва може бути вироб-вільним англійською мовою з обов'язковим збереженням розширенням-ня CSS)

• images.

Вибір сайту на PHP невипадковий, тому що PHP - це серверний мова і код програми виконується безпосередньо на сервері, користувач не бачить код про-грами на мові програмування PHP.

3.3 Проектування розміщення ресурсів проекту

Проектування робимо з урахуванням використання MVC (Model-View-Controller - Модель-Представлення-Контролер, див. рис. 3.2) - способу побудо-ви структури додатку, метою якого є відділення бізнес-логіки від призначеного для користувача інтерфейсу. В результаті, додаток легше масштабується, тесту-ється, супроводжується і звичайно ж реалізується.

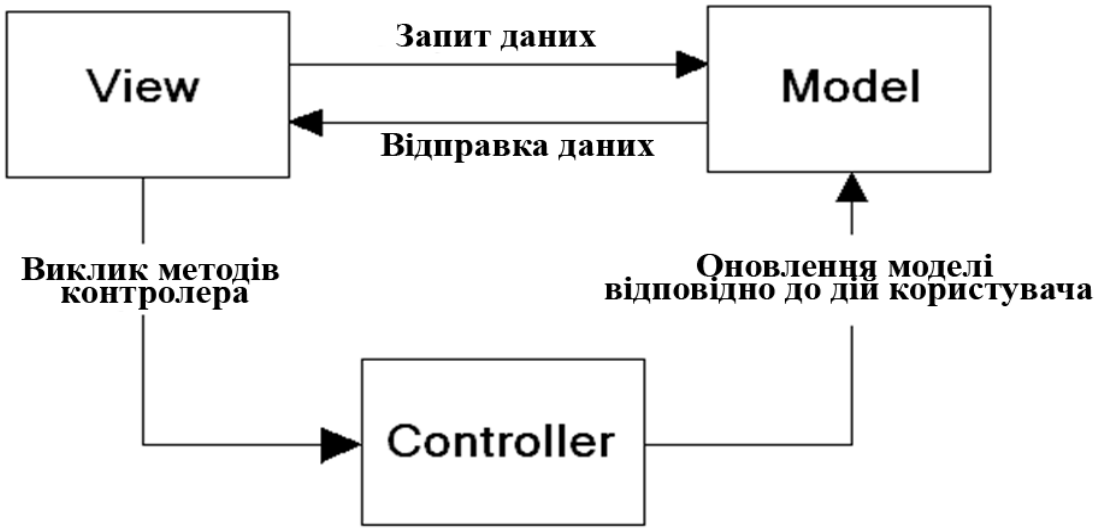

Рис 3.2. Модель-Представлення-Контролер

Типову послідовність роботи MVC-додатку можна описати таким чином:

1. При заході користувача на веб-ресурс, скрипт ініціалізації створює екземпляр програми та запускає його на виконання.

2. При цьому відображається вид, скажімо головної сторінки сайту.

3. Додаток отримує запит від користувача і визначає конкретний контролер і дію. У разі головної сторінки, виконується дія за замовчуванням (index).

4. Додаток створює екземпляр контролера і запускає метод дій в якому, наприклад, міститися виклики моделі, що зчитують інформацію з бази даних.

6. Після цього, дія формує уявлення з даними, отриманими з моделі і виводить результат користувачеві.

Модель - буде містити бізнес-логіку програми та вмикати методи вибірки (це можуть бути методи ORM), обробки (наприклад, правила валідації) і надавати конкретні даних.

Модель не повинна безпосередньо взаємодіяти з користувачем. Всі змінні, що відносяться до запиту користувача повинні оброблятися в контролері. Модель не повинна генерувати HTML або інший код відображення, який може змінюватися в залежності від потреб користувача. Такий код повинен оброблятися в видах. Одна і та ж модель, наприклад: модель автентифікації користувачів може використовуватися як в призначеній для користувача, так і в адміністративній частині програми. В такому випадку можна винести загальний код в окремий клас і успадковуватися від нього, визначаючи в спадкоємців специфічні для додатків методи.

Подання (вид). Використовуємо для завдання зовнішнього відображення даних, отриманих з контролера і моделі.

Види містять HTML-розмітку і невеликі вставки PHP-коду для обходу, форматування і відображення даних: «чи не повинні безпосередньо звертатися до бази даних; цим повинні займатися моделі; чи не повинні працювати з даними, отриманими із запиту користувача; це завдання має виконувати контролер; можливо безпосередньо звертатися до властивостей і методів контролера або моделей, для отримання готових до висновку даних».

Види зазвичай поділяють на загальний шаблон, що містить розмітку, загальну для всіх сторінок (наприклад, шапку і підвал) і частини шаблону, які використовують для відображення даних, що виводяться з моделі або відображення форм введення даних.

Контролер - сполучна ланка, що з'єднує моделі, види і інші компоненти в робоче додаток. Контролер відповідає за обробку запитів користувача. Контролер не повинен містити SQL-запитів. Їх краще тримати в моделях. Контролер не повинен містити HTML і інший розмітки. Її варто виносити в види.

У добре спроектованому MVC-додатку контролери містять тільки кілька десятків рядків коду. Логіка контролера досить типова і велика її частина виноситься в базові класи.

3.4 Створення бази даних для зберігання інформації

Створюємо базу даних на базі MySQL. У базі даних створюємо необхідні для роботи сайту таблиці для зберігання:

1) даних зареєстрованих користувачів (див. рис.3.3);

	#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐	1	id	int(10)		UNSIGNED	Нет	Нем		AUTO_INCREMENT	Изменить Удалить Ещё
☐	2	name	varchar(32)	utf8_general_ci		Да	NULL			Изменить Удалить Ещё
☐	3	login	varchar(32)	utf8_general_ci		Нет	Нем			Изменить Удалить Ещё
☐	4	password	varchar(32)	utf8_general_ci		Нет	Нем			Изменить Удалить Ещё
☐	5	email	varchar(64)	utf8_general_ci		Нет	Нем			Изменить Удалить Ещё
☐	6	birthday	date			Да	NULL			Изменить Удалить Ещё
☐	7	gender	varchar(6)	utf8_general_ci		Да	NULL			Изменить Удалить Ещё

Рис. 3.3. Приклад таблиці даних зареєстрованих користувачів

2) даних про права доступу другого рівня (покупці, див. рис. 3.4);

	#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно	Действие
☐	1	user_id	int(10)		UNSIGNED	Нет	Нем			Изменить Удалить Ещё

Рис. 3.4. Приклад таблиці покупців

3) даних про права доступу третього рівня (редактори);

4) даних про права доступу четвертого рівня (адміністратори);

5) інформації про товари;

6) інформації про замовлення;

7) даних по оплаті;

8) даних про статуси замовлень;

9) дані про способи доставки.

3.5. Розробка програмної частини сайту

У програмній частині реалізуємо алгоритми роботи сайту з урахуванням системи контролю доступу. У своїй роботі активно використовуємо SQL запити реалізовані в коді програм. Для роботи з MySQL постійно використовуємо систему CRUD (Створення Редагування Зміна Видалення).

Створюємо системи реєстрації та авторизації користувача з урахуванням перевірки введених даних, захисту даних від введення шкідливого коду (див. рис. 3.5).[Додаток А]

Файл Кодировка Синтаксис Поиск Найти и Заменить Настройки

```
<?PHP
  session_start();
$pass   = strip_tags($_POST["Password"]);
$name   = strip_tags($_POST["Name"]);
$login  = strip_tags($_POST["Login"]);
$date   = strip_tags($_POST["Date"]);
$pochta = strip_tags($_POST["Email"]);
$gender = strip_tags($_POST["Gender"]);

$pass = md5(yaiyuhf972ZA37huuin . $pass);

include "db.php";

$str = "
INSERT INTO `comrade`(`name`, `login`, `password`, `email`, `birthday`, `gender`) VALUES ('$name'
  ,'$login','$pass','$pochta','$date','$gender')

";
$result = $db->query($str);
if( $result ) {
  $_SESSION['message'] = 'Registration completed successfully';
    header('Location: ../auth.php');
} else {$_SESSION['message'] = '!!! Registration failed login or mail is already taken';
    header('Location: ../reg.php');
  }
```

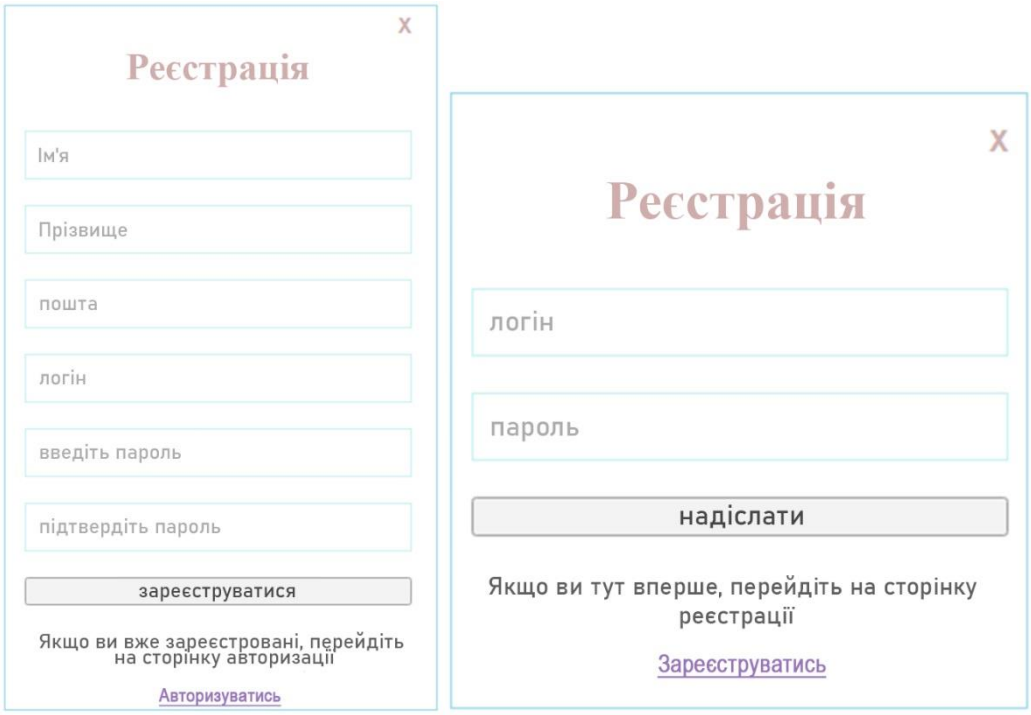

Рис. 3.5. Авторизація та реєстрація даних [Додоток Б]

Використовуємо систему шифрування md5 з додаванням спеціального набору символів («солі») для безпечного зберігання в базі даних (див. рис. 3.6).

id	name	login	password	email	birthday	gender
5	bobi	bobi	5e81702f69b0d6ca70c02cb710483f8b	ff@rr.ua	2021-04-24	Муж
17	boss	boss	e3e65e65cb128dcd05475d7369e1a9f0	xxx@xx.ua	0021-05-08	Муж
60	fnf	fnf	5e81702f69b0d6ca70c02cb710483f8b	fnf@xx.ua	2021-05-07	Муж
67	bobas	bobas	425322530fb768ba16f876237919d6fa	bobas@oo.ru	2021-05-07	Муж
73	abc1	abc1	5e81702f69b0d6ca70c02cb710483f8b	dudu@ee.ua	2021-05-07	Муж
77	bobsi	bobsi	5e81702f69b0d6ca70c02cb710483f8b	bobsi@kuku.ua	2021-05-06	Муж
80	abc3	abc3	5e81702f69b0d6ca70c02cb710483f8b	abc3@bobo.ua	2021-05-07	Муж

Рис 2.6. База даних MySQL

Навіть якщо зловмисник отримає доступ до бази MySQL, він не зможе використовувати дані зашифрованого пароля.

Обробляємо дані, отримані з форми авторизації, виконуємо запит до бази даних і перенаправляємо користувача (див. рис. 3.7).

```php
<?php
session_start();
//header("Content-Type: text/html; charset=utf-8");
$login = strip_tags($_POST['login']);
$pass = strip_tags($_POST['pass']);

$pass = md5(yaiyuhf972ZA37huuin . $pass);

include "db.php";

$str = "
SELECT * FROM comrade
WHERE login = '$login' AND password = '$pass';
";

$result = $db->query( $str );
$user = $result->fetch_assoc();
if( $user ){
  $_SESSION['user'] = $user;
  header('Location: ../boss.php');
} else {$_SESSION['message'] = '!!! Username or password is incorrect';
    header('Location: ../auth.php');
  }
```

Рис. 3.7. Обробка даних

Реалізуємо контроль доступу до блоків, сторінок, кнопок і їх видимість для користувачів різного рівня (див. рис. 3.8).[Додаток В]

```php
<?php
session_start();
$user = $_SESSION['user'];

if( empty( $_SESSION['user'] ) ) {//if the user is not logged in
  header("Location: auth.php");//go to the login page
}

$id = $user['id'];
include "controller/db.php";

$sql = "SELECT * FROM `boss` WHERE id = $id";
$result = $db->query( $sql );//this returns a result set
$result = $result->fetch_assoc();////this returns either NULL or the resulting series as an
  associative array

if( empty($result)){//if the user is not an editor, transfer him to the main page
  header("Location: edit.php");
}
$title = "Editor";
include "header.php";
?>
  <div>
    <?php include "controller/messages/session_message.php"?>
  </div>
<?php
include "controller/sql_query/editors.php";//displaying a table of authors
include "controller/sql_query/articles.php";//displaying a table of goods
include "controller/sql_query/users.php";//displaying a table of users
?>
<br><br><br>
<?php
include 'footer.php';
?>
```

Рис. 3.8. Реалізація контролю доступу для користувачів різного рівня

Далі в проекті реалізуються механізми управління групами товарів, редагування інформації про товари, видалення товарів, система управління доставкою товару, система управління статусом виконання замовлення та інше.

3.6 Установка платіжної системи на сайт

Відповідно до політики, встановленої провайдерами систем онлайн-платежів:

• сайт повинен бути публічним, всі його сторінки розміщені на одному домені, а посилання повинні відкриватися без помилки 404;

• на сайті має бути максимум інформації про продукт;

• важливо подбати про контент, політиків і угодах.

На нашому сайті буде інформація:

• повна назва компанії;

• достовірне і зрозумілий опис товару / послуги;

• контакти: телефон, Email , месенджери;

• умови доставки та повернення товару;

• договір публічної оферти або угоду користувача;

• політика конфіденційності і політика використання cookie-файлів.

Перший етап - створити акаунт в платіжній системі. Він буде особистим кабінетом (ЛК), де можна стежити за всіма операції, виводити зароблені кошти, управляти настройками проекту.

Після реєстрації потрібно створити касу. Каса - це по суті онлайн-точка прийому платежів для бізнесу. Їй в системі присвоюється унікальний ID-номер. В одному акаунті може бути необмежена кількість кас, так що ми можемо підключати відразу кілька проектів і працювати з ними через ЛК.

Активація каси відбувається після того, як сайт пройде додаткову модерацію - етап, на якому команда платіжної системи перевіряє відповідність проекту вимогам платіжного сервісу. Як швидко пройде перевірка, залежить від трьох чинників - готовність сайту, тип бізнесу, методи оплати.

Якщо команда модерації знаходить проблеми на сайті або в документації, то прийом платежів не буде активований і вони попросять усунути недоліки. Коли все буде готово, платіжна система активується.

Попередні кроки - це більше організаційні моменти, але у підключення оплати на сайт є і технічний етап - інтеграція платіжної кнопки і / або форми оплати на наш ресурс.

Є кілька варіантів підключитися до сервісу прийому платежів - за допомогою **API, SDK** або плагіна для **CMS.**

Ми можемо заздалегідь вибрати зручний спосіб інтеграції або зробити це вже в процесі підключення (після консультації з техподдержкой платіжного сервісу). Зробити це можна самостійно, або за допомогою команди розробників: все залежить від того, як саме ми будемо проводити інтеграцію. Interkassa пропонує три варіанти підключення:

Плагін для CMS - підійде для інтернет-магазину створеного на базі Wordpress, Opencart або іншої платформи. Для підключення досить завантажити розширення для цієї системи і просто встановити його на сайт через панель адміністратора. Інструкції по установці зазвичай йде в комплекті з модулем. Налаштувати плагін зможе навіть фахівець без технічних знань, тому таку інтеграцію часто вибирає невеликі проекти, у яких немає штатної it-команди.

API - метод інтеграції використовують в двох випадках:

• сайт (наш варіант): його створила команда розробників з нуля, а не на базі якоїсь CMS;

• платформа працює на CMS, але конкретно для цієї платформи немає готового плагіна. У цьому випадку завдання бізнесу - розмістити на сайті спеціальну кнопку оплати. Коли покупець натисне на неї, в платіжну систему повинен відправитися запит на створення платежу і необхідні для цього параметри. Таку кнопку можна додати на кожну картку товару, або тільки на сторінку з кошиком.

• Підключення по API вимагає більше часу і ресурсів, тому тут вже буде важко без it-фахівця. Це мінус, але в той же час таке рішення більш гнучке і до-

зволяє бізнесу кастомизировать деякі настройки. Наприклад, підключаючись до платіжної стстеме по API, продавець може вибирати режим роботи - стандартний або прихований.

SDK - це по суті все та ж API-інтеграція, але для неї вже є готовий код, зібраний комплект інструментів для реалізація тієї чи іншої функції. У Interkassa теж є свій toolkit для розробників - SDK для проектів на PHP.

Підключаючись за допомогою SDK ми можемо отримати все ті ж платіжні переваги, що і завдяки API-інтеграції - гнучкість налаштувань, можливість кастомізувати окремі функції системи під себе. Але технічно організувати прийом платежів на сайті простіше і швидше з SDK, тому що розробникам потрібно писати менше коду.

3.7 Аудит сайту

1. Проводимо дослідження і оцінку рівня захищеності інформаційних систем компанії на поточний момент:

• Проводимо тести системи реєстрації та авторизації. Якщо в результаті тестів не вдається отримати доступ до закритих ресурсів сайту - система контролю доступу надійно захищена. У разі хоча б одного випадку нелегального проникнення, записуємо проблему і усуваємо.

• Перевіряємо поля введення тексту на введення скриптів і вразливість. У разі виявлення уразливості, усуваємо і тестуємо знову.

• Оцінюємо потенційні збитки, якщо кіберзагрози будуть реалізовані. І оцінюємо вартість наслідків кібератак. Формуємо резерв коштів на випадок виникнення проблеми з інтернет ресурсом і створюємо алгоритм вирішення можливих ситуацій.

• Розробляємо заходи щодо захисту систем та захисту інформації. Створюємо систему резервного копіювання ресурсу, бази даних, виконуємо вищевказані тести на регулярній основі.

• Оцінюємо рентабельність і розробляємо заходи кібербезпеки для мінімізації ризиків.

3.8 Висновки до третього розділу

В результаті проведеної роботи створено модель системи контролю безпеки даних на прикладі створення ресурсу - сайту інтернет магазину.

На сайті реалізована система реєстрації і авторизації користувача з визначенням рівня доступу і контрольованого надання інформації. При роботі з персональними даними на сайті реалізована система шіфрова-ня md5 з додаванням спеціального набору символів, що робить процеси отримання та обробки надійними.

На різних рівнях доступу до сайту прошивки на мові PHP відправляють запити до бази даних MySQL, в якій зберігаються всі дані сайту.

На сайті реалізована система CRUD (Створення Читання Редагування Видалення). Операції можна виконувати виключно користувачами з відповідними правами доступу, з метою захисту від несанкціонованого зміни даних.

З метою підтримки безперервності роботи сайту та прискорення відновлення даних, реалізована система щоденного резервного копіювання ресурсу.

В результаті проведення аудиту сайту, всі виявлені проблеми безпеки усунені. Тестування проводяться на регулярній основі. Також з огляду на підключення платіжної системи на сайті, проводиться додаткова модерація представниками платіжної системи.

Завдання по створенню системи контролю доступу до персональних даних користувача реалізована повністю.

ВИСНОВКИ

Сучасні технології розвиваються ще більш стрімкішими темпами кожного дня, розробникам доводиться шукати нові способи якісного захисту і контролю інформації. Саме тому щороку все більше зростає необхідність організацій в побудові якісної інформаційної системи обробки даних.

В роботі було розглянуто сукупність методів, заходів і засобів для запобігання несанкціонованого доступу до ресурсів, для забезпечення цілісності даних. Були проаналізовані методи і засоби шифрування даних, те як можна авторизуватись за допомогою SSH протоколу, захистити персональні дані за допомогою двофакторної автентифікації та як можна авторизуватись через фізичний USB-ключ носій.

Зроблений аналіз методів нормалізації бази даних та як з їх допомогою можна оптимізувати базу даних, і захистити її скориставшись ефектом нормалізації. Розглянуто способи захисту від найпоширеніших атак на веб сервіси SQL та PHP ін’єкцій, за допомогою програмних засобів, які дозволяють за допомогою спеціальних функцій захистити свій веб-сервіс.

Досліджені також методи виявлення проблемних місць системи безпеки підприємства.

В результаті проведеної роботи створено модель системи контролю безпеки даних на прикладі створення ресурсу - сайту інтернет магазину.

СП**ИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Про інформацію: Закон України від 02.10.1992 р. // Відомості Верховної Ради України. –1992.–No 48.–Ст.650.

2. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.). - М.: Права человека, 2009.

3. Контроль доступа (информатика) [Електронний ресурс] // ВикипедиЯ. – 2020. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0).

4. Что такое SSH? [Електронний ресурс] // Freehost.ua. – 2018. – Режим доступу до ресурсу: https://freehost.com.ua/faq/wiki/chto-takoe-ssh/.

5. *Курило А. П., Мамыкин В. Н.* Обеспечение информационной безопасности бизнеса. С. 291-294.

6. https://www.cloud.net.ua/osobennosti-token-avtorizacii-i-oblast-ih-primeneniya

7. Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» // Відомості Верховної Ради України. –2012. – No 1556-VII

8. Authentication essentials [Електроннийресурс]: -Режим доступу до ресурсу: https://searchsecurity.techtarget.com/definition/authentication

9. Cyber Security requires strong UX [Електронний ресурс] :- Режим доступу до ресурсу: https://hackernoon.com/cyber-security-requires-an-important-ingredient-strong-ux-d0727a0c076

10. Брижко В.М.Організаційно-правові питання захисту персональних даних:автореф.дис...канд.юрид.наук:12.00.07-адміністративне право і процес,інформаційне право/В.М.Брижко.–Ірпінь,2004.–20с.

11. Інформаційне право та правова інформатика у сфері захисту персональних даних : моногр./В.Брижко,М.Гуцалюк,В.Цимбалюк,М.Швець;за ред.М.Швеця.–К.:НДЦПІ АПрН України,2006.–450с.

12.Бєляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення:моногр./К.І.Бєляков.–К.:КВІЦ,2008.–576с

13. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : моногр./І.В.Арістова.–Х.:Вид-во Університету внутрішніх справ,2000.–368с.

14. Рижова В.А. Проектування і дослідження комплексних систем безпеки. СПб . : НІУІТМО, 2012. 157с.

15. Фаткулин А. Н. АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ [Електронний ресурс] / А. Н. Фаткулин // ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ. – 2011. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/analiz-sovremennyh-sistem-kontrolya-i-upravleniya-dostupom/viewer.

16. Васильев Д. А. Подход к модернизации системы защиты информации в образовательных учреждениях среднего общего полного образования [Електронний ресурс] / Д. А. Васильев // Курский государственный университет. – 2017. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/podhod-k-modernizatsii-sistemy-zaschity-informatsii-v-obrazovatelnyh-uchrezhdeniyah-srednego-obschego-polnogo-obrazovaniya/viewer

17. Ярославцев О. С. Разработка системы управления доступом и охранной сигнализации гостинничного комплекса [Електронний ресурс] / О. С. Ярославцев // Пермский государственный технический университет. – 2015. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/razrabotka-sistemy-upravleniya-dospupom-i-ohrannoy-signalizatsii-gostinichnogo-kompleksa-new-star/viewer

18. Зыков В. Д. Структура программного обеспечения системы защиты рабочего места обработки персональных медицинских данных [Електронний ресурс] / В. Д. Зыков // Структура программного обеспечения системы защиты рабочего места обработки. – 2019. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/struktura-programmnogo-obespecheniya-sistemy-zaschity-rabochego-mesta-obrabotki-personalnyh-meditsinskih-dannyh/viewer.

19. Хованец В. А. Адаптация информационных систем управления университетам требованиям закона о защите персональных данных [Електронний ресурс] / В. А. Хованец, П. В. Смолим // Доклады ТУСУРа. – 2010. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/adaptatsiya-informatsionnyh-sistem-upravleniya-universitetom-trebovaniyam-zakona-o-zaschite-personalnyh-dannyh/viewer.

20. Грибова В. В. Защита персональных данных в системе контроля и управления доступом (СКУД) [Електронний ресурс] / Василина Вячеславовна Грибова // Международный научный журнал "Символ науки". – 2016. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-sisteme-kontrolya-i-upravleniya-dostupom-skud/viewer.

21. Німченко, Т. В. Алгоритм виявлення несанкціонованого витоку персональних даних мережевими каналами [Текст] / Т. В. Німченко, І. М. Мужик, А. І. Мужик // Вісник інженрної академії України. — 2014. — No 3–4. — С. 199–203.

22. Філоненко, С. Ф. Система попередження витоку персональніх даних мережевими каналами [Текст] / С. Ф. Філоненко, І. М. Мужик, Т. В. Німченко // Ukrainian Scientific Jornal of Information Security. — 2014. — Vol. 20, No 3. — P. 279–285.

23. Німченко, Т. В. Критерій визначення з переліку даних тих, що відносяться до категорії персональні [Текст] / Т. В. Німченко // Вісник інженерної академії України. — 2015. — No 1. —С. 199–202

24. Марков, А. П. Проблемы и решения по защите персональных данных в информационных системах персональных данных [Текст] / А. П. Марков, Б. И. Сухинин // Компьютерная безопасность. — 2009. — No 5. — С. 20–27

25. Инсайдерские угрозы в России 2009 [Электронный ресурс]. — 2009. — Режим доступа: \www/URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pd

26. INFOBEZEXPO — международная выставкаконференция[Электронный ресурс]. — 2013. — Режим доступа: \www/URL: http://infobezexpo.ru

27. Сулавко, А. Е. Технологии защиты от внутренних угроз информационной безопасности [Текст] / А. Е. Сулавко // Вестник СибАД. — 2011. — No 1(19) — С. 45–51.

28. Аверченков, В. И. Формализация процесса выбора состава средств обеспечения безопасности на объекте защиты [Текст] / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин // Вестник компьютерных и информационных технологий. — 2010. — No 11. — С. 45–50.

29/ Гуцалюк, М. Інформаційна безпека України: нові загрози та організація протидії [Текст] / М. Гуцалюк // Правова інформатика. — 2004. — No 3. — С. 37–41.

30. Прокоф’єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів [Текст] / Д.М. Прокоф’єва // Український центр інформаційної безпеки. 2008. – С.123-128.

31.Ткачук Т. Формування системи інформаційної безпеки бізнесу [Текст] / Т.Ткачук // Бізнес і безпека, 2009. - No4. – С.19-23.

32. Волков Я. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации [Текст] / Я.Волков // Финансовая газета, 2006. – No34. – С.15.

33. Voron, M. (2016). Prava liudyny v Interneti[Human rights on the Internet]. Retrieved April 1, 2018, from http://nmcio.ippo.kubg.edu.ua/?p=2213(in

Ukrainian)[Ворон, М. (2016). ПравалюдинивІнтернеті. Актуально на 01.04.2018. URL: http://nmcio.ippo.kubg.edu.ua/?p=2213].

34. Tarasenko, L. L. (n. d.).Tsyfrove seredovyshche yak mistse zdiisnennia prav intelektualnoi vlasnosti[The digital environment as a place of realization of intellectual property rights]. Retrieved April1, 2018, from https://goo.gl/HYymYb(in Ukrainian)[Тарасенко, Л. Л. (н. д.). Цифрове середовище як місце здійснення прав інтелектуальної власності. Актуально на 01.04.2018. URL: https://goo.gl/HYymYb]

35. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс]. –Режим доступу : http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7 C00499C02.

36. Розслідування 12016040730000533. [Електронний ресурс] // Єдиний реєстр досудових розслідувань : [веб-сайт]. –Режим доступу : http://www.gp.gov.ua/ua/erdr.html.

37. FIPS PUB 140-2. Security Requirements for Cryptographic Modules // Federal Information Processing Standards Publication 140-2, U.S. Department of Commerce,05/2001.

38. БєловС.В., МартиненкоС.В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики [Електронний ресурс].– Режим доступу : http://www.itsway.kiev.ua/pdf/Model-CA_Risks.pdf.

39. ПогореловБ.А. Об определении основных криптографических понятий / Б.А.Погорелов, А.В.Черемушкин, С.И.Чечета // Доклад на конференции "Математика и безопасность информационных технологий" (МаБИТ-03, МГУ, 23-24 октября 2003 г.)

ДОДАТОК А

Обробка авторизації

```
<?php
session_start();
//header("Content-Type: text/html; charset=utf-8");
$login = strip_tags($_POST['login']);
$pass = strip_tags($_POST['pass']);

$pass = md5(yaiyuhf972ZA37huuin . $pass);

include "db.php";

$str = "
SELECT * FROM comrade
WHERE login = '$login' AND password = '$pass';
";

$result = $db->query( $str );
$user = $result->fetch_assoc();
if( $user ){
  $_SESSION['user'] = $user;
  header('Location: ../boss.php');
} else {$_SESSION['message'] = '!!! Неправильний логін або пароль';
    header('Location: ../auth.php');
  }
```

ДОДАТОК Б

Файл обробки реєстрації

```
<?PHP
  session_start();
$pass   = strip_tags($_POST["Пароль"]);
$name   = strip_tags($_POST["Ім'я"]);
$login  = strip_tags($_POST["Логін"]);
$date   = strip_tags($_POST["Дата"]);
$pochta = strip_tags($_POST["Пошта"]);
$gender = strip_tags($_POST["Стать"]);

$pass = md5(yaiyuhf972ZA37huuin . $pass);

include "db.php";

$str = "
INSERT INTO `comrade`(`name`, `login`, `password`, `email`, `birthday`, `gender`)
VALUES ('$name','$login','$pass','$pochta','$date','$gender')


";
$result = $db->query($str);
if( $result ) {
  $_SESSION['message'] = ' Реєстрація пройшла вдало';
      header('Location: ../auth.php');
} else {$_SESSION['message'] = '!!! Реєстрація не вдалась логін або пошта вже
зайняті';
    header('Location: ../reg.php');
  }
```

ДОДАТОК В

Реалізація контролю доступу до блоків , сторінок, кнопок і їх видимість для користувачів різного рівня

```
<?php
session_start();
$user = $_SESSION['user'];

if( empty( $_SESSION['user'] ) ) { //if the user is not logged in
  header("Location: auth.php"); //go to the login page
}

$id = $user['id'];
include "controller/db.php";

$sql = "SELECT * FROM `boss` WHERE id = $id";
$result = $db->query( $sql ); //this returns a result set
$result = $result->fetch_assoc();////this returns either NULL or the resulting series as an associative array

if( empty($result)){//if the user is not an editor, transfer him to the main page
  header("Location: edit.php");
}
$title = "Editor";
include "header.php";
?>
  <div>
```

```
    <?php include "controller/messages/session_message.php"?>
  </div>
<?php
include "controller/sql_query/editors.php"; //displaying a table of authors
include "controller/sql_query/articles.php"; //displaying a table of goods
include "controller/sql_query/users.php"; //displaying a table of users
?>
<br><br><br>
<?php
include 'footer.php';
?>
```