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

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ та контролю доступу до вебсайту «Електронний паспорт здоров'я студентів»
Назва теми

КвРКБ.170153.17.02.14 ПЗ
Шифр

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

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Назва

Виконав: студентка IV курсу, група КБ–17–1 _____ О.О. Савіцька
Підпис Ініціали, прізвище

Керівник _____ К.В. Молодецька
Підпис, дата Ініціали, прізвище

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

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

« 7 » червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Завідувач кафедри _____

_____

5 • 01 2021 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Савіцькій Ользі Олегівні

Прізвище, ім'я, по батькові студента

1 Тема роботи Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ та контролю доступу до вебсайту «Електронний паспорт здоров'я студентів»

Керівник роботи Молдецька К. В. д.т.н.

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

Затверджено наказом ректора університету від 05 02 2021р. № 11 додаток 9

2 Строк подання студентом роботи на кафедру: _____

3 Вихідні дані до роботи проведення дослідження об'єкта захисту, методів та засобів захисту від вебатак, класифікація загроз і каналів витоку інформації навчально-наукової лабораторії, розробити комплексний підхід до виявлення та захисту інформації, визначення шкідливого трафіку та захист вебсайту від DDoS-атак

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Дослідження та опис об'єкта захисту, аналіз об'єкта захисту, розробка комплексної системи захисту, реалізація роботи

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «Організаційна структура лабораторії», «Структурні доступи до різних рівнів інформації», «Розташування камер спостереження у приміщеннях лабораторії», «Схема даних вебсайту Epass», «Принципові схеми алгоритмів по визначенню початку атаки і виділенню шкідливого трафіку», «Топологія фільтрації трафіку мережі».

6 Консультанти розділів курсового проекту (роботи)

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

7 Дата видачі завдання 05 лютий 2021 р.

КАЛЕНДАРНИЙ ПЛАН

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

Студент _____ О.О. Савіцька
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ К.В. Молодецька
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ та контролю доступу до вебсайту «Електронний паспорт здоров'я студентів».

Автор роботи: Савіцька Ольга Олегівна.

Керівник роботи: Молодецька Катерина Валеріївна.

Обсяг – 70 с., 17 рис., 2 додатка, 26 джерел.

Графічна частина: 18 презентаційних слайдів, 6 плакатів.

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, АТАКИ НА ВЕБСАЙТ, ЗАХИСТ ТА КОНТРОЛЬ ДОСТУПУ ДО ВЕБСАЙТУ.

Метою роботи є створення комплексної системи захисту об'єкта, виявлення витоків інформації у лабораторії, дослідження вразливостей вебсайту, захист вебсайту, на основі моделювання можливих кібер-атак на нього.

У роботі було досліджено та проаналізовано типові проблеми інформаційної безпеки в кібернетичному просторі, особливу увагу було зосереджено на вразливостях наявного вебсайту.

В рамках кваліфікаційної роботи було модифіковано наявний вебсайт на основі фреймворку Laravel, з метою захисту та коректного функціонування. Реалізовано контроль доступу до вебсайту.

Підпис студента 

Дата 4.06.2021

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1		Завдання на дипломний проект	1	
А4		2		Анотація	1	
А4		3	КвРКБ.170153.17.01.14 ПЗ	Аудит системи захисту лабораторії ХНУ та контролю доступу до вебсайту «Електронний паспорт здоров'я студентів» Пояснювальна записка	1	
А2		4	КвРКБ.170153.17.01.14 ПЗ	Організаційна структура лабораторії Схема структурна	1	
А2		5	КвРКБ.170153.17.01.14 ПЗ	Структурні доступи до різних рівнів інформації Схема структурна	1	
А2		6	КвРКБ.170153.17.01.14 Е8	Розташування камер спостереження у приміщеннях лабораторії Схема структурна	1	

КвРКБ.170153.17.01.14 ВП

Зм.	Арк.	№ Докум.	Підп.	Дата
Розробив		Савіцька О.О.		
Перев.		Молодецька К.В.		
Н. контр.		Муляр І.В.		
Затв.		Кльоц Ю.П.		

Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ

Літера	Аркуш	Аркушів
н	1	2

ХНУ, КБ-17-1

зона	Позиц	Позначення	та контролю доступу	Кільк.	Прим.
	7	КвРКБ.170153.17.01.14 Е8	до вебсайту «Електронний	1	
			паспорт здоров'я студентів»		
			Схема структурна		
	8	КвРКБ.170153.17.01.14 Е8	Принципові схеми початку	1	
			алгоритмів по визначенню		
			атаки і виділенню		
			шкідливого трафіку		
			Алгоритм роботи		
	9	КвРКБ.170153.17.01.14 Е8	Топологія фільтрації	1	
			трафіку мережі		
			Схема структурна		

ЗМІСТ

ВСТУП

Актуальність теми кваліфікаційної роботи зумовлена стрімким розвитком інформаційних технологій, що спричиняє загрозу конфіденційності, цілісності та доступності інформації, як професійної так і особистої.

Важливість кібербезпеки зростає. Принципово, що наше суспільство є більш технологічним, ніж будь-коли раніше, і немає жодних ознак того, що ця тенденція сповільниться. Усім відомо, що техніка робить за нас велику частину роботи, а згодом зможе замінити навіть ряд популярних професій.

Зараз дуже багато особистої інформації публікується в інтернеті, що може призвести до крадіжки конфіденційних даних. Не говорячи вже про такі мережі як “Instagram”, “Facebook”, “Twitter”, за допомогою яких ми знаємо де мешкає людина, у які супермаркети ходить, з ким спілкується, та навіть в якому ресторані вечеряє по п’ятницям.

Конфіденційна інформація, така як номери соціального страхування, дані кредитної картки та реквізити банківських рахунків, тепер зберігаються в хмарних сховищах, таких як Dropbox або Google Drive.

Наші гаджети завжди з нами, коли ми говоримо про якусь річ, залізні друзі вже шукають яку саме рекламу нам продемонструвати. З одного боку це зручно, але з іншого, постає питання, чи не можуть використати таку інформацію зловмисники у власних цілях.

Реєструючись на різних сайтах ми залишаємо інформацію про себе, яку теж можна використати проти нас.

Тому потрібно бути уважними з тим який контент робити публічним.

Під загрозу кібератак, підпадає не тільки особиста інформація, а і професійна. Ви щодня працюєте з комп’ютерними системами.

Це спричинено зростанням хмарних сервісів. Але через їх недосконалу захищеність, ми маємо незліченну кількість загроз кібербезпеки, яких не було кілька десятиліть тому.

Все більшу популярність набирають напади на компанії в найрізноманітніших галузях, за останні п’ять років вони подвоїлися. Зазвичай великі компанії сплачують немалі кошти для того, щоб захиститися від кіберзлочинців [1].

А чи потрібна взагалі думати про інформаційну безпеку не великим фірмам? Ходить міф, нібито кіберзлочинці полюють на корпорації з величезні оборотами, а скромних підприємців не помічають. Таке припущення невірне. За статистикою невеликі і середні підприємства найчастіше стають жертвами кіберзлочинців. Це пояснюється трьома фактами:

- дуже малий відсоток людей проводить перевірку на наявність вразливостей у додатках;
- більшість програм, що застосовуються в корпоративному середовищі, мають як мінімум одну серйозну вразливість;
- дуже великі збитки від кібератак.

Мало кому відомі усі аспекти кібербезпеки, саме тому люди нею нехтують, та потрапляють у скрутні ситуації.

Усі підприємства, незалежно від розміру, повинні забезпечити, щоб усі співробітники розуміли загрози кібербезпеки та знали способи їх пом'якшення. Це повинно включати регулярне навчання та основу для роботи, яка має на меті зменшити ризик витоку даних або порушення даних.

Отже, розглянемо основні поняття сутності кібербезпеки.

Під інформаційною безпекою розуміється захист об'єкта (держави, юридичної особи, фізичної особи) у сфері інформації, де інформаційне поле - це сукупність інформаційної інфраструктури (тобто інформація та її обробка), суб'єкти, що збирають, формують , розповсюдження та використання інформації, а також система регулювання суспільних відносин, що виникають [2].

Основною метою інформаційної безпеки є захист інформаційних активів від загроз та вразливостей, яким може бути піддана організація . У сукупності загрози та вразливості становлять інформаційний ризик. Забезпечення досягнення цілей безпеки та зменшення ризиків принесе користь організації, сприяючи:

- безперервності бізнесу;

– операційній ефективності;

– економічній ефективності.

Хороша програма з кібербезпеки повинна не тільки захищати внутрішні дані, які підприємство вважає конфіденційними, але має і захищати інформацію, що ідентифікує особисті дані своїх клієнтів. Прикладом персональної інформації є номер соціального страхування споживача, номер посвідчення водія, навіть його електронна адреса [3].

Основними характеристиками інформаційної безпеки є:

– доступність – дає змогу отримати приватну інформацію, тим хто має дозвіл на доступ до неї, наприклад, коли клієнт просить переглянути його або її профіль;

– цілісність – дає змогу переконатися, що дані є надійними та захищеними від несанкціонованих змін, фальсифікацій, знищення або втрати;

– конфіденційність – забезпечує захист від несанкціонованого ознайомлення.

Шифрування та встановлення паролів – це способи забезпечити дотримання заходів безпеки щодо конфіденційності.

Процес ІБ – це складний процес, який полягає у взаємодії сутностей, які беруть участь у процесі забезпечення ІБ:

1. Вимоги для забезпечення інформаційної безпеки.

2. Захищена інформація.

3. Загрози що можуть погіршити характеристики захищеної інформації до неприйнятного рівня.

4. Механізми та засоби протидії загрозам.

5. Інформаційна система, в якій обробляється захищена інформація.

6. Зовнішні умови, які сприяють або гальмують процес забезпечення ІБ.

7. Об’єкти, що обслуговуються інформаційною системою і пов’язані із захищеною інформацією.

За рахунок того що компоненти інформаційної безпеки, а також можливості організації змінюються, вимоги щодо забезпечення інформаційної безпеки та складу контрзаходів можуть мінятись.

1 ХАРАКТЕРИСТИКА НАВЧАЛЬНО-НАУКОВОЇ ЛАБОРАТОРІЇ МЕДИКО-ПСИХОЛОГІЧНИХ ДОСЛІДЖЕНЬ ХНУ – ЯК ОБ'ЄКТА ЗАХИСТУ

1.1 Дослідження та опис об'єкта захисту

Навчально-наукова лабораторія медико-психологічних досліджень ХНУ займається наданням студентам та викладачам комплексних та ґрунтовних медико-психологічних знань з метою створення суспільно-корисних навчальних та наукових результатів, забезпечення якісної освітньої підготовки майбутніх фахівців, та науково-педагогічних кадрів вищої кваліфікації, а також наданням інших послуг студентам для створення їм комфортних і зручних умов у виконанні ними навчальних планів.

Основні завдання лабораторії:

1. Покращення підготовки студентів шляхом забезпечення гармонійного поєднання практичних та наукових видів та методів медико-психологічної допомоги.

2. Проведення медико-психологічних та психофізіологічних досліджень з питань покращення якості життя та збереження здоров'я людини, надання науково-методичної та практичної допомоги учасникам навчально-виховного процесу з питань медико-психологічної та соціально-педагогічної підтримки.

3. Надання просвітницьких послуг викладачам і студентам ХНУ.

4. Надання освітніх послуг за соціально-реабілітаційним та оздоровчим напрямком для потреб громадян.

5. Медико-психологічна допомога щодо збереження психічного здоров'я студентів, а також в адаптації студентів-першокурсників до навчання у ВНЗ засобами тренінгової діяльності.

6. Забезпечення взаємодії навчальної теорії і практичних навичок в процесі професійної підготовки за соціономічним профілем студентів ХНУ.

7. Створення умов для творчої самореалізації студентської молоді в процесі навчання та підготовки до практичної діяльності.

8. Проведення навчальних і виробничих практик студентів.

9. Проведення студентських науково-дослідних робіт.

10. Експериментальна робота у природних умовах на основі поєднання освітньо-виховного процесу з науковими дослідженнями з метою підвищення якості підготовки фахівців.

Лабораторія розташовується у студентському гуртожитку на нульовому поверсі, що знаходиться за адресою Інституцька 14/2.

Уся внутрішньо нормативна документація лабораторії, персональні дані співробітників та пацієнтів знаходяться у паперовому вигляді.

Інформація про стан здоров'я пацієнтів, правила внутрішнього трудового розпорядку, посадові інструкції, положення про оплату праці, положення про преміювання, заяви згоди співробітників на збір персональних даних, заяви згоди пацієнтів на збір персональних даних знаходяться і в електронному і в паперовому вигляді.

Дані встановлені під час дослідження пацієнтів та діагнози пацієнтів знаходяться лише в електронному вигляді.

Варто зазначити, що лабораторія займається покращенням здоров'я пацієнтів, тому співробітники лабораторії мають доступ до секретної інформації пацієнтів.

В умовах карантину, роботу з пацієнтами в основному виконують дистанційно. За допомогою вебсайту «Eppas-xeol.com.ua», уся інформація здобута в процесі досліджень зберігається там.

1.2 Структура навчально-наукової лабораторії медико-психологічних досліджень ХНУ

Навчально-наукова лабораторія медико-психологічних досліджень ХНУ є невеликою за розмірами та кількістю працівників.

Існує міф що кібератаки здійснюються тільки на великі компанії, але насправді це не так. Більшість серйозних фірм не нехтують своєю безпекою та вкладають великі суми грошей для забезпечення надійного захисту. Також, в наш час існує велика конкуренція, що теж є досить вагомою причиною для кібернападу. Саме це спонукає кіберзлочинців все частіше завдавати шкоди невеликим компаніям.

У лабораторії працює 11 працівників.

Керівник лабораторії – Янцаловський Олександр Йосипович, займається проведенням дослідних робіт, забезпечує розробку заходів, спрямованих на покращення технічного стану техніко-економічних показників, керує робітниками лабораторії, організовує дослідження нових методів дослідження здоров'я.

Старший лаборант – Повстюк Олена Юріївна, займається розробкою та аналізом психологічних тестів. Проводить регулярні тестування пацієнтів, на основі отриманих даних слідкує за динамікою психологічного здоров'я пацієнтів.

Старший лаборант – Леус Олена Віталіївна, проводить аналіз результатів впровадження програми самозбереження та займається розробкою програм самозбереження для кожного пацієнта окремо.

Старший лаборант – Соловей Алла Вікторівна, займається фізичним здоров'ям пацієнтів, проводить заміри антропометричних показників, відслідковує їх динаміку, проводить фізичне тестування пацієнтів та підбирає для кожного пацієнта вправи для покращення фізичного здоров'я.

Лаборант – Лушевська Олена Сергіївна, займається науково дослідницькою роботою, відповідає за проведення наукових семінарів та конференцій.

Веброзробник – Савіцька Ольга Олегівна, займається розробкою та підтримкою сайту «Epass.xeol.com.ua». Працює над наповненням, розробкою нових модулів та аналітикою сайту.

Системний адміністратор – Голованов Іван Петрович, займається встановленням і обслуговуванням комп'ютерної техніки, забезпечує коректну роботу програмного забезпечення, забезпечує роботу мережі лабораторії.

Головний бухгалтер – Петришина Ніна Василівна, займається веденням бухгалтерських звітів, начисленням заробітної плати працівникам, розрахунками податкових звітів.

Бухгалтер – Василюк Інна Петрівна, займається виплатами заробітної плати співробітникам.

Прибиральниця – Петрук Галина Іванівна, проводить сухе та вологе прибирання лабораторії один раз на два дні.

Електрик – Галицький Віктор Михайлович, працює в галузі електрики і електротехніки, що займається монтажем, експлуатацією або ремонтом електротехніки.

Сантехнік – Іваніцький Віктор Григорович, здійснює монтажні роботи із встановлення систем опалення, водопостачання та каналізації

У лабораторії кожен працівник відноситься до окремого відділу. Відділів існує 5 (рис. 1.1) :

- відділ адміністрації;
- технічний відділ;
- лаборанти;
- бухгалтерія;
- технічний персонал.

Рисунок 1.1 – Організаційна структура лабораторії

Розглянемо структурні доступи до різних рівнів інформації навчально-наукової лабораторії медико-психологічних досліджень ХНУ.

Структурні доступи до різних рівнів інформації представлені на рис.1.2.

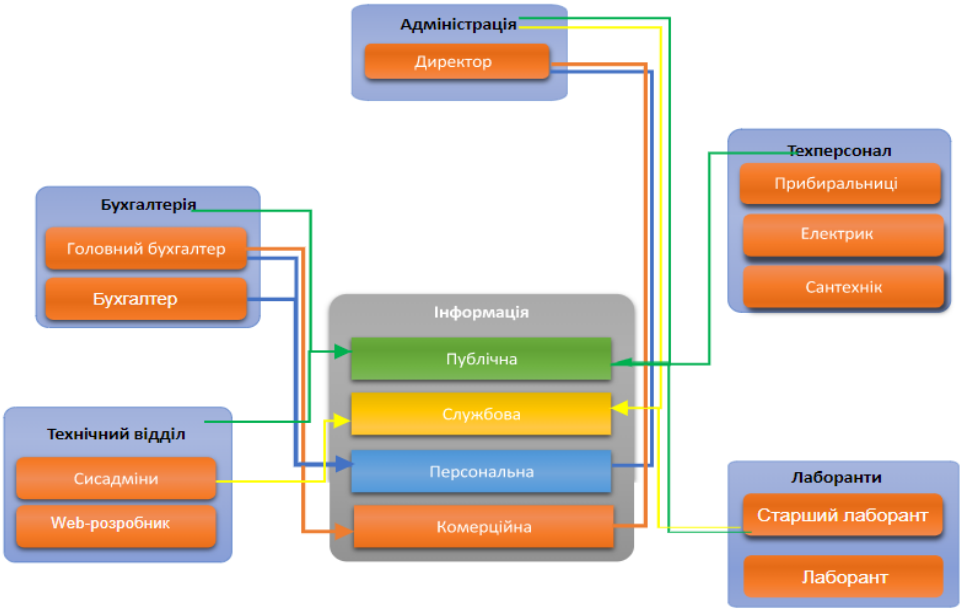


Рисунок 1.2 – Структурні доступи до різних рівнів інформації

З рис. 1.2 видно, що кожен підрозділ має певні особливості доступу до інформації.

Відділ адміністрації, а саме керівник лабораторії, має доступ до всіх типів інформації(публічної, службової, персональної, комерційної).

У технічному відділі, саме системний адміністратор та веброзробник мають доступ до публічної, службової та персональної інформації.

Лаборант, а саме усі старші лаборанти мають доступ до публічної та персональної інформації.

Бухгалтерія як і всі інші підрозділи має доступ до публічної інформації, головний бухгалтер, який відповідає за всі фінансові операції має доступ і до персональних даних співробітників і до комерційної інформації.

Технічний персонал, а саме прибиральниця має доступ лише до публічної інформації.

1.3 Опис технічного і інформаційного забезпечення навчально-наукової лабораторії медико-психологічних досліджень ХНУ

У лабораторії наявне таке обладнання:

- 2 ноутбуки;
- 2 персональних комп'ютери;
- 1 БФП (принтер, сканер, ксерокс 3 в 1);
- 1 стаціонарний телефон;
- 2 роутери;
- телевізор Samsung QE50Q60TAUXUA;
- 5 велотренажерів;
- 2 дошки для спини.

В якості операційної системи на усіх ноутбуках та ПК використовується ліцензійний Windows 10.

Крім програмного забезпечення, яке є необхідним для працівника, щоб виконати свої посадові обов'язки є ще перелік програмних продуктів:

- Microsoft Office 2016;
- Powerpoint 2016;
- Антивирус Avast;
- Adobe Reader 8;
- Yandex;
- Google Chrome;
- Opera;
- WinRAR;
- Total Commander;
- Phpstorm.

Також сайт «Epass.xeol.com.ua» знаходится на локальному сервері лабораторії, що включає в себе комплекс програм – Apache, MySQL, PHP.

1.4 Дослідження методів та засобів захисту від вебатак

На жаль, на сьогоднішній день, вебдодатки є найбільш доступними для кібератак. Зазвичай вебдодатки містять в собі дуже багато конфіденційної інформації, наприклад базу клієнтів, базу товарів, результати тестувань, опитувань, деякі навіть паспортні дані користувачів, тому дуже важливо забезпечити безпеку таких додатків належним чином.

Атака на вебдодаток

Існують різні вебдодатки, наприклад інтернет магазини, CPM, вебпошта, соціальні мережі, освітні програми, біржі, банківські додатки, розважальні програми, замовлення їжі та багато інших. Для розробки вебдодатків девелопери використовують комбінації серверного сценарія (Node,Python, PHP, ASP та багато інших), а також скриптів на стороні клієнта (JavaScript, HTML та інші). Проте і серверна і клієнтська частини мають вразливості, які і призводять до кібератак.

Причому атаки можуть бути не тільки складними, а й дуже простими, наприклад маніпулювання даними в url, щоб викликати вразливості в додатку.

Є три основних види вебатак:

- PHP injection;
- SQL injection;
- XSS.

PHP injection – це вид атак, робота якого полягає в виконанні стороннього коду на стороні сервера [4].

Найбільш розповсюдженими є введення SQL ін’єкцій і атаки виду Cross-Site Scripting (XSS).

Атаки типу SQL injection працюють за рахунок розміщення шкідливого коду, який може зруйнувати всю базу даних. Найчастіше такі атаки відбуваються коли у користувача запрошуються якісь дані для введення. Користувач-зловмисник замість введення реальних даних відправляє інструкцію SQL, яка запускається у базі даних.

XSS атаки – це атаки на основі DOM дерева, які відбуваються шляхом виконання шкідливих скриптів на стороні клієнта. Особливістю цієї атаки є те що у

сервера не буде можливості виявити таку атаку, так як атака відбувається на стороні клієнта. В основному, такі атаки відбуваються тому що розробники не змогли написати безпечний код. Зараз дуже розповсюдженою є атака скримінга платіжних карт(DPCS)[5].

Засоби захисту від вебатак представляють собою комплекс мір захисту, які направленні на забезпечення доступності роботи вебдодатків за рахунок захисту їх від різних типів атак [6].

Основними методами захисту від таких атак є:

- захист від PHP injection;
- захист від SQL injection;
- захист від XSS;
- захист від DDOS-атак;
- перевірка відповідності даних до стандартів протоколів;
- механізми перевірки трафіку на основі нейронних мереж;
- сигнатурний та репутаційний аналіз;
- проведення аудиту нових скриптів;
- ведення звітності про трафік сайту.

1.5 Постановка задачі

Метою кваліфікаційної роботи є своєчасне виявлення та недопущення зовнішніх і внутрішніх загроз, захист від вебатак, забезпечення захищеності лабораторії.

Для досягнення поставленої мети в кваліфікаційній роботі необхідно вирішити наступні задачі:

- виявити всі структурні підрозділи досліджуваного об’єкта;
- проаналізувати доступи до інформації;
- провести аналіз носіїв;
- вказати всі загрози;
- виявити найбільш вразливі місця лабораторії;

- виявити якій загрозі потрібно надати найбільше уваги;
- розробити модель комплексної системи захисту;
- розробити модель охоронної та пожежної сигналізації об’єкта;
- розробити політики інформаційної безпеки;
- виявити вразливості вебсайту;
- розробити контроль доступу до вебсайту;
- зробити висновки проведеної роботи.

2 АНАЛІЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НАВЧАЛЬНО-НАУКОВОЇ ЛАБОРАТОРІЇ МЕДИКО-ПСИХОЛОГІЧНИХ ДОСЛІДЖЕНЬ ХНУ

2.1 Аудит інформаційної безпеки, цілі і задачі аудиту

З метою оцінки реального стану захищеності ресурсів інформаційної системи і визначенню здатності протистояти як зовнішнім так і внутрішнім загрозам проводять аудит інформаційної безпеки.

Аудиту інформаційної безпеки – це комплекс аналітичної оцінки стану інформаційних систем та пошук можливих загроз.

Аудиту інформаційної безпеки має кілька етапів:

- Прийняття рішення про необхідність аудиту – рішення приймається безпосередньо всередині організації.
- Збір даних. IT – спеціалісти збирають, сортують та аналізують актуальні дані та передають для подальшої обробки.
- Аналіз даних – спеціалісти порівнюють отримані дані про інформаційну систему, порівнюють їх з актуальними стандартами і роблять висновки.
- Написання звіту-включає в себе загальну оцінку підприємства, список проблем з детальними рекомендаціями [7].

Основними цілями аудиту є:

- аналіз поточного рівня захищеності персональних даних;
- виявлення недоліків і аналіз ефективності існуючої політики, стандартів і процедур;
- виявлення існуючих вразливостей і ризиків;
- перевірка існуючих заходів безпеки з операційних та адміністративних питань і забезпечити відповідність до стандартів безпеки;
- формування звіту для спеціалістів з забезпечення інформаційної безпеки.

Часто, не дивлячись на тип підприємства, його задачі цілі та діяльність, аудит інформаційної захищеності включає такі робочі аспекти:

- знання працівників про захист даних;
- права на доступ до баз даних та серверів колективного використання;
- налаштування мережевих пристроїв;
- аутентифікація;
- система зберігання та передачі даних;
- наявність ліцензії;
- робота антивірусного ПЗ.

Отже, комплексний аудит інформаційної безпеки дуже важливий, так як він допомагає виявити наскільки система захисту є ефективною. А також якісна аналітика дасть змогу підібрати найефективніші методики захисту даних та знизити витрати на них.

2.2 Аналіз системи захисту інформації навчально-наукової лабораторії медико-психологічних досліджень ХНУ

Усім відомо що розвиток інформаційних технологій зараз відбувається надзвичайно швидко, нових технологій дуже багато, багато інформації знаходиться в електронному вигляді. У зв'язку з цим все більше зростає потреба у забезпеченні якісного захисту інформації [8].

Під поняттям «Аналіз системи захисту інформації» розуміють комплексний аналіз фактів, подій, явищ та процесів пов'язаних з проблемами захисту інформації.

Аналітична робота повинна включати елементи прогнозування можливих загроз [9].

Аналіз системи захисту інформації містить такі задачі:

- аналіз можливих каналів витоку інформації;
- оцінка ефективності наявних заходів спрямованих на закриття каналів витоку інформації;
- оцінка дій робітників підприємства для вирішення завдань захисту інформації.

Для проведення аналізу системи захисту інформації досліджуваного об’єкта будемо слідувати такому алгоритму дій:

- сформуємо перелік джерел конфіденційної інформації, що наявна у лабораторії;
- розподілимо конфіденційну інформацію за ступенем її цінності;
- сформуємо перелік носіїв на яких зберігається конфіденційна інформація;
- визначимо ступінь обізнаності працівників щодо поведінки з конфіденційними даними;
- виявимо внутрішні та зовнішні загрози;
- виявимо потенційних зловмисників, які можуть бути зацікавлені в отриманні конфіденційної інформації;
- проаналізуємо коректність заходів, що зараз виконуються у лабораторії для захисту конфіденційної інформації.

Провівши дослідження наявної конфіденційної лабораторії було виявлено, що лабораторія містить загальну конфіденційну (інформація про своїх співробітників, пацієнтів), а також внутрішню нормативну документацію.

До загальної інформації входять:

- загальна база пацієнтів;
- план розвитку лабораторії;
- персональні дані співробітників;
- персональні дані пацієнтів;
- інформація про стан здоров’я пацієнтів;
- дані встановлені під час дослідження пацієнтів;
- результати проходження психологічних тестів;
- результати анкетувань пацієнтів;
- діагнози поставлені пацієнтам.

Внутрішня нормативна документація лабораторії включає:

- правила внутрішнього трудового розпорядку;
- посадові інструкції;
- положення про оплату праці;

- положення про преміювання;
- заяви згоди співробітників на збір персональних даних;
- заяви згоди пацієнтів на збір персональних даних.

Проведемо розподіл цінності інформації, що зберігається у лабораторії. Для оцінки будемо використовувати такі критерії:

- оцінка головних цілей системи і врахування всіх її головних сторін діяльності;
- критичність;
- простота.

За проведеними дослідженнями було встановлено розподіл цінності інформації за шкалою від 1 до 5 (табл. 1.1).

Таблиця 1.1 – Розподіл цінності інформації

Вид інформації	**Оцінка**
1	**2**
Загальна база пацієнтів	5
План розвитку лабораторії	5
Персональні дані співробітників	5
Персональні дані пацієнтів	5
Інформація про стан здоров’я пацієнтів	5
Дані встановлені під час дослідження пацієнтів	5
Результати проходження психологічних тестів та анкетувань	5
Діагнози поставлені пацієнтам	5
Правила внутрішнього трудового розпорядку	3
Посадові інструкції	3

Продовження таблиці

1	2
Положення про оплату праці та преміювання	4
Заяви згоди співробітників та працівників на збір персональних даних	4
База даних	5

Носіями конфіденційної інформації є флеш-носії та оптичні диски співробітників лабораторії. Також було виявлено що у лабораторії не ведеться резервне копіювання даних, що є дуже великим недоліком, так як є великий ризик втрати даних.

Провівши бесіду з працівниками лабораторії було з'ясовано, що обізнаність про поводження з конфіденційною інформацією вони мають, проте у лабораторії відсутні політики інформаційної безпеки.

Також потрібно проводити бесіди з співробітниками, щоб вони завжди мали достатній рівень знань, щоб запобігти втраті чи витоку інформації.

Відносно інформаційної системи всю сукупність загроз можна розбити на зовнішні і внутрішні, кожна з яких, в свою чергу, ділиться на навмисні та випадкові загрози, які бувають явними і прихованими.

До зовнішніх загроз підприємства відносять викрадення матеріальних засобів і цінностей особами, що не є робітниками цієї фірми, промислове шпигунство, незаконні дії конкурентів, здирство з боку кримінальних структур, будь-які дії з цінними паперами, агресивну купівлю акцій підприємства зовнішнім інвестором.

До зовнішніх загроз можемо віднести:

- відвідувачів;
- представників з комунальних організацій (енергопостачання, теплопостачання та водопостачання);
- конкуренти або особи які працюють за дорученням;
- особи, які потрапили до приміщення без дозволу;
- пацієнтів та хакерів.

До внутрішніх загроз відносять такі, як низька кваліфікація фахівців, розголошення власними співробітниками конфіденційної інформації, неефективна робота служби фінансової або економічної безпеки й осіб, неефективне фінансове планування та управління активами, неефективне управління ринком акцій підприємства.

Найбільшу небезпеку, як правило, становлять зовнішні загрози, які не піддаються виявленню і прогнозуванню. У той же час усунення внутрішніх загроз належить до компетенції органів управління підприємством.

Перейдемо до внутрішніх порушників. Їх можна поділити на:

- основний персонал (найбільш небезпечний тип порушників);
- тимчасовий персонал об’єкта;
- співробітників організацій, що мають право на збір інформації.

Серед них виділимо такі категорії персоналу:

- співробітники відділів розробки;
- користувачі;
- технологічний персонал (інженери);
- технічний персонал (прибиральниці, електрики, сантехніки);
- керівники відділів.

З розвитком технологій потенційних зловмисників стає все більше. Для лабораторії потенційними зловмисниками можуть бути: конкуренти, звільнені працівники, недобросовісні пацієнти, необізнані працівники, невідомі хакери.

2.3 Класифікація загроз і каналів витоку інформації навчально-наукової лабораторії медико-психологічних досліджень ХНУ

Витік інформації – це неправомірне розповсюдження даних, що виходять за межі кола довірених осіб, які зберігали ці дані, іншими словами це володіння чужою інформацією, незалежно від способу, яким було отримано ці дані. Важливо розуміти що витік даних може відбутись як через зовнішні так і через внутрішні канали, тому потрібно прийняти міри захисту так, щоб вони охопили всі області.

Причини витоку інформації можуть бути навмисні та ненавмисні. Ненавмисні виникають, наприклад, у випадках коли співробітники випадково надіслали лист з конфіденційними даними іншому одержувачу. Навмисні виникають коли зловмисник свідомо намагається здобути конфіденційну інформацію.

Канали витоку інформації – це шлях інформації, який вона проходить від джерела інформації до приймача, який в процесі витоку інформації отримує конфіденційну інформацію. У разі на прийнятих заходів захисту інформації, зловмисники можуть використати будь-які канали, а якщо захист був передбачений, тоді будуть використовуватись найменш захищені канали.

За типом реалізації канали витоку інформації поділяються на фізичні та інформаційні.

Найпоширенішими фізичними каналами є канали витоку інформації пов'язані з документообігом та збереженням конфіденційних даних в архіві.

Розглянемо фізичні канали витоку інформації. Витік інформації відбувається при несвоєчасному знищенні документів, в результаті відкритого доступу до місць в яких перебуває інформація, в результаті перехоплення документа після закінчення друку, відсутність або неправильність знищення документів при здійснені переїзду.

На досліджуваному об'єкті план розвитку лабораторії, персональні дані співробітників, персональні дані пацієнтів, та внутрішньо нормативна документація до якої виходять: правила внутрішнього трудового розпорядку, посадові інструкції, положення про оплату праці, положення про преміювання, заяви згоди співробітників на збір персональних даних, заяви згоди пацієнтів на збір персональних даних зберігаються в архіві. Ключ від архіву має головний бухгалтер та директор. При потенційній втраті або викраденні ключа, доступ до цих даних може отримати зловмисник.

Заяви згоди співробітників на збір персональних даних та заяви згоди пацієнтів на збір персональних даних зберігаються в електронному вигляді на локальному комп'ютері директора. Потенційно зловмисник може дізнатись або підібрати пароль входу у систему локального комп'ютера та отримати доступ до

конфіденційних даних. Також при поломці або уражені вірусами комп'ютера інформація буде пошкоджена, або знищена без можливості її відновити.

Ще є загроза витоку інформації через оптичний канал, так як вікна лабораторії знаходяться на нульовому поверсі і на вікнах відсутні завіси, то будь-хто може спостерігати за діями у лабораторії. Крім цього стіни кабінету виготовлені з газоблоку, що загрожує витоку інформації через акустичний канал. Потенційний зловмисник може підслухати розмову, яка відбувається в кабінеті.

Інформаційні канали витоку інформації

Інформаційні канали витоку дуже різні та здатні пропускати через себе великі обсяги даних.

Основними з них є:

- витоки по вебканалах;
- витоки через корпоративну пошту;
- витоки через мобільні пристрої;
- витоки через носії інформації.

Можливі витоки з серверних компонентів, якщо наявні вразливості в корпоративних технологія і процесах:

- не контрольованість привілейованих користувачів;
- не організована фільтрація доступу до систем збереження та обробки даних.

Витоки інформації при використанні мобільних пристроїв чи ПК зумовлена такими факторами:

- втрата пристрою на якому знаходиться конфіденційна інформація;
- можливість відключити агент моніторингу та відправити дані які його цікавлять будь-яким способом;
- відсутність контролю за встановленими додатками можливе встановлення стеганографічного чи криптографічного ПЗ і передача даних навіть через агента моніторингу;
- підключення до ПК на якому зберігається конфіденційна інформація носіїв (usb-модем, зовнішній жорсткий диск, флеш носії і подібних) з метою несанкціонованого копіювання інформації.

Також є ряд причин за яких можливі витоки через вебканали [10]

- вигрузка даних на хмарні сервіси;
- відправка даних через web-mail;
- відправка даних за допомогою сервісів передачі повідомлень;
- організація тунелю до інших ресурсів і вигрузка через нього конфіденційної інформації.

Під час досліджень проведених у лабораторії було виявлено ряд вразливостей.

Насамперед, було виявлено загрозу витоку інформації при використанні ПК. Так як конфіденційні дані зберігаються на локальному комп'ютері директора, то є потенційна загроза витоку інформації шляхом приєднання до ПК носія (usb-модему, зовнішнього жорсткого диску, флеш носіїв) та копіювання інформації. Також, користувач який має права адміністратора може відключити агента моніторингу і відправити будь-які дані. На додачу, на комп'ютері відсутній антивірус, що може призвести до пошкодження або знищення інформації.

Було проведено перевірку вразливості вебсайту і виявлено такі вразливості:

- відсутність захисту від CSRF атак;
- відсутність захисту від SQL-ін'єкцій;
- відсутність перевірки вхідних даних;
- відсутність захисту від XSS атак;
- відсутність захисту даних сесії;
- відсутність обробки помилок і виключень обробка помилок;
- відсутність захисту файлів що підключаються;
- відсутність захисту від DDoS-атак;
- відсутність регулярного Backup;
- використання старої версії PHP;
- невикористання PDO.

2.4 Висновки

Отже, для того щоб мати змогу протистояти як зовнішнім так і внутрішнім загрозам потрібно провести аудит інформаційної безпеки, який дає змогу реально оцінити стан захищеності підприємства. Під час проведення аудиту досліджуваного об’єкта було сформовано перелік джерел конфіденційної інформації, розподілено конфіденційну інформацію за ступенем її цінності, сформовано перелік носіїв конфіденційної інформації, виявлено внутрішні та зовнішні загрози, виявлено потенційних зловмисників, виявлено існуючі вразливості та ризики, знайдено потенційні канали витоку інформації. Можемо зробити висновок, що стан захищеності лабораторії є незадовільним, а заходи які виконуються у лабораторії для захисту конфіденційної інформації є недостатніми.

3 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ НАВЧАЛЬНО-НАУКОВОЇ ЛАБОРАТОРІЇ МЕДИКО-ПСИХОЛОГІЧНИХ ДОСЛІДЖЕНЬ ХНУ

3.1 Правовий захист інформації

Основним аспектом комплексної системи захисту інформації є правовий захист інформації.

Формою правового захисту інформації є захист інформації, який спирається на статті Конституції та законів держави, положень кримінального та цивільного кодексів, а також інших нормативно-правових документів щодо захисту інформації та інформаційних відносин.

Правовий захист регулюється на міжнародному та державному рівні. На державному рівні регулюється державними нормативно-правовими актами.

Фундаментом правового захисту інформації є національне інформаційне право, а його предметом виступають суспільні відносини, які виникають в результаті встановлення режимів і форм обігу інформації, а також реалізації інформаційних прав, правового статуту суб'єктів і формування їх правомірної поведінки та зв’язків [11].

Метою правового захисту інформації є збереження державної та професійної таємниці, збереження конфіденційності документованої інформації щодо законодавства.

Будь-яка документована інформація підлягає захисту, якщо її неправомірне використання може нанести збитки її користувачу, власнику або іншій особі.

До структури інформаційної безпеки входять:

- закони України;
- кримінальний кодекс України [12] та господарський [13];
- Конституція України [14];
- державні стандарти та нормативні акти;
- постанови Кабінету Міністрів України та укази Президента України.

Правовий захист націлений на вирішення таких проблем:

- захист державних секретів;
- захист персональних даних;
- захист комерційної таємниці;
- боротьба з кіберзлочинністю;
- контроль безпеки інформаційних систем;
- страхування інформаційних систем.

Правовий режим інформації це порядок регулювання, який відображений в комплексі правових засобів, які характеризують взаємодію дозволів та заборон, які утворюють особливе спрямування регулювання.

До правового режиму входить:

- право доступу до інформації;
- право поширення і надання інформації;
- право володіння інформацією;
- майнові права на носії, на яких зберігається інформація.

На досліджуваному об’єкті зберігається чимала кількість конфіденційних даних (персональні дані співробітників та пацієнтів, інформація про стан здоров’я пацієнтів, дані встановлені під час дослідження пацієнтів, результати проходження психологічних тестів та анкетувань, діагнози поставлені пацієнтам та інші), тому дуже важливо належним чином впровадити правовий захист інформації.

Насамперед, потрібно розробити політики інформаційної безпеки та ознайомити всіх працівників з ними, регулярно проводити конференції на яких потрібно нагадувати про наслідки недотримання правових норм захисту. Також потрібно отримати авторське право на існуючий вебсайт.

Політики інформаційної безпеки це комплекс правил, принципів та заходів, якими керуються співробітники організації з метою захисту інформаційних ресурсів [15].

Розробка ефективної системи інформаційної безпеки

Для створення ефективної системи інформаційної безпеки повинні бути розроблені:

– концепція інформаційної безпеки (визначає в цілому політику, її принципи та цілі) [16];

– стандарти (правила і принципи захисту інформації по кожному конкретному напрямку) [17];

– процедура (опис конкретних дій для захисту інформації при роботі з нею: персональних даних, порядку доступу до інформаційних носіїв, систем і ресурсів);

– інструкції (докладний опис того, що і як робити для організації інформаційного захисту та забезпечення наявних стандартів).

Всі вищезазначені документи повинні бути взаємопов’язані і не суперечити один одному.

Перейдемо до розробки політик інформаційної безпеки навчально-наукової лабораторії медико-психологічних досліджень ХНУ

Політика безпеки розповсюджується на навчально-наукову лабораторію медико-психологічних досліджень ХНУ в цілому та повинна бути використана для усіх інформаційних ресурсів та процесів.

Директор навчально-наукової лабораторії медико-психологічних досліджень ХНУ затверджує політику та інші нормативні документи, контролює та приймає рішення щодо фінансування проектів з інформаційної безпеки.

У навчально-науковій лабораторії медико-психологічних досліджень ХНУ необхідно визначити:

– визначений перелік інформаційних ресурсів, які потребують першочергово захисту;

– забезпечений відповідний рівень інформаційної безпеки для цілісності, доступності та конфіденційності інформації в залежності від класифікації цієї інформації;

– доступ до вебсайту має бути заснований на рольовій моделі доступу;

– потрібен постійний контроль актуальності та ефективності впроваджених рішень щодо забезпечення інформаційної безпеки;

– ознайомлення усіх працівників зі своїми посадовими інструкціями;

− доведення до працівників відповідальності. яку вони несуть за розголошення конфіденційних даних;

− щорічне тестування вебсайту спрямоване на виявлення вразливостей;

− регулярне проведення конференцій спрямованих на пояснення наслідків за недотримання закону України «Про захист персональних даних» [18].

3.2 Інженерно-технічний захист навчально-наукової лабораторії медико-психологічних досліджень ХНУ

3.2.1 Засоби пожежної сигналізації

Основним етапом установки на об’єкті засобів пожежної безпеки є монтаж пожежної сигналізації. На кожному підприємстві пожежна сигналізація є безпосереднім впровадженням даної системи на об’єкт, її установку, наладку і здачу в експлуатацію. Так як монтаж сигналізації вимагає високих знань і особливого професіоналізму в області протипожежних систем, він є невід’ємною частиною кожного підприємства і забезпечує високу безпеку не тільки життя і здоров’я співробітників, але і матеріальних благ, що знаходяться на об’єкті.

Система пожежної сигналізації являє собою складний комплекс технічних засобів, службовців для своєчасного виявлення спалаху і евакуації людей. Як правило, пожежна сигналізація інтегрується в комплекс, який об’єднує системи безпеки і інженерні системи будівлі, забезпечуючи достовірною адресною інформацією системи оповіщення, пожежогасіння, димовидалення, контролю доступу [19]. При виникненні пожежі сповіщувач виявляє підвищення температури, дим та полум’я і повідомляє про це на приймально-контрольний прилад. Після цього включаються звукові і світлові сповіщувачі, які повідомляють про спрацьовування сповіщувача. При цьому додатково може активуватися димовидалення, пожежогасіння, аварійного управління ліфтами, оповіщення людей про пожежу.

Для забезпечення цілковитої безпеки рекомендуємо встановити складні систему пожежної сигналізації з запам’ятовуванням і можливістю перегляду всіх

подій, що відбувалися. Всі події, що відбувалися фіксуються в спеціальній пам’яті панелі і можуть бути виведені на друк або на екран із зазначенням дати і часу події.

Система оповіщення є невід’ємною і дуже важливою частиною будь-якої пожежно-охоронної системи. При виявленні вогнища пожежі необхідно, перш за все, запобігти паніці, попередити людей, вивести їх з небезпечних місць, а для цього необхідна система оповіщення населення.

Доцільно встановити пожежну сигналізацію у всіх приміщеннях, особливо в тих де працюють сервери та зберігаються конфіденційні дані.

3.2.2 Засоби охоронної сигналізації та відеонагляду

Камери спостереження дуже важлива складова комплексу захисту підприємства. Вони можуть стати єдиним джерелом інформації про її ураження, несанкціонований доступ або засобом встановлення подій. Всі приміщення де відбувається обробка та накопичення службової, персональної та комерційної інформації повинні бути захищені відеоспостереженням.

Незаконне проникнення може спричинити за собою самі різні негативні наслідки від крадіжки матеріальних цінностей до нанесення шкоди здоров’ю осіб, які перебувають на об’єкті. Переваги сучасних охоронних технологій дозволяють убезпечити квартиру, гараж, офіс від протиправних дій, а також мінімізувати можливість несанкціонованого доступу на територію підприємств.

За планом лабораторії є доцільним розташування 7-ми камер спостереження у приміщеннях де відбувається обробка інформації, а саме: кабінет директора, зали для розробників, кабінет бухгалтерії та у коридорі перед вхідними дверима. Таким чином, накопичуючи відеозаписи, можна відтворити події і з’ясувати джерела витоку інформації або їх спроби. Розташування камер спостереження у приміщеннях компанії представлено на рис. 3.1.

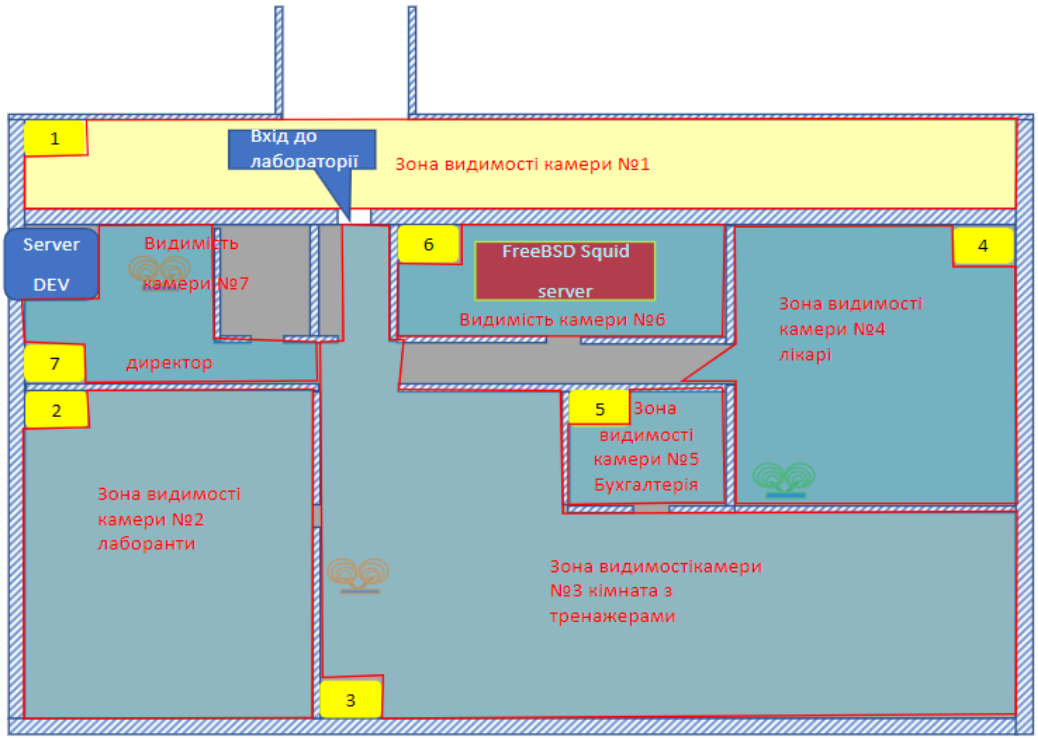


Рисунок 3.1 – Розташування камер спостереження у приміщеннях лабораторії

Враховуючи характеристики, ціну та якість в компанію доцільно придбати камери моделі Atis AI-223FE, яка має такі характеристики:

- роздільна здатність: Full HD (1920x1080 пікселів);
- об’єктив: 1.44mm (кут огляду 180˚);
- стиснення відео: кодек H.264;
- частота кадрів: 25fps;
- підтримка P2P (робота без статичної IP адреси);
- запис відео: безперервний;
- підтримка SD: micro SD карту до 64 ГБ;
- ІК підсвітка: 10м;
- протокол бездротової мережі WiFi 802.11 b/n;
- живлення: DC 5V 300mA;
- розміри: 75x75x120mm;
- вага: 0.3kg;
- робоча температура: від –10°C до +50°C 95%RH

3.2.3 Оцінка звукоізоляції об’єкта захисту

Захист акустичної інформації є одним з найважливіших завдань в комплексному захисті безпеки об’єкта. Для того щоб перехопити мовну інформацію потенційний зловмисник може скористатись багатьма портативними засобами акустичної розвідки, які дадуть змогу перехопити мовну інформацію по акустичному, електроакустичному та віброакустичному каналах[20].

Для ослаблення акустичних сигналів встановлюється звукоізоляція приміщень, яка націлена на локалізацію джерел акустичних сигналів всередині приміщень.

Звукоізоляція є головним методом захисту акустичної інформації.

Головною умовою звукоізоляції – відношення шуму за межами приміщення не може бути вище допустимого значення. Це дає змогу виключити виділення мовних сигналів на тлі природних шумів. Завдання звукоізоляції – не дозволити звуку пройти крізь стіну приміщення [22].

Звукоізоляція будь-якої будівельної конструкції визначається товщиною, чим більша товщина конструкції, тим важче звуковим коливанням її розхитати. Звукоізолююча здатність конструкцій оцінюється значенням індексу звукоізоляції. Вимірюється індекс звукоізоляції в дБ. Звукоізолюючий є матеріали, які здатні відбивати звук, наприклад цегла, бетон, гіпсокартон та інші.

За нормативними вимогами до звукоізоляції внутрішніх огороджувальних конструкцій лікарень, було визначено що індекс приведеного рівня ударного шуму перекриття між кабінетами лабораторії допустимий в межах 60-63 дБ [22].

За нормативними значеннями звукоізоляція вікон має становити не менше 65 дБ.

Приміщення лабораторії знаходиться на нульовому поверсі, несучі стіни виготовлені з цегли, а стіни між кабінетами виготовлені з газоблоків. Вікна у лабораторії є звичайні, пластикові, з однокамерними склопакетами, без шумопоглинання. Вхідні двері лабораторії є звичайними щитовими дверима, які облицьовані фанерою з двох сторін. Міжкімнатними дверима є типові дерев’яні двері без прокладки. Варто взяти до уваги, що лабораторія розташована на

нульовому поверсі, неподалік від спортивного майданчика, це означає, що рівень потрапляння шуму до приміщення буде підвищеним.

Двері та вікна вважаються найслабкішими звукоізолюючими конструкціями, так як вони мають меншу поверхневу щільність та містять важко ущільнювальні отвори і щілини, в порівняні з стінами та міжповерховими перекриттями. Так, як у лабораторії встановлені звичайні дерев'яні двері без прокладок, з наявними щілинами між підлогою та дверима, можемо зробити висновок, що вони не задовольняють умовам захисту за табл. 3.1

Таблиця 3.1 – Звукоізоляція звичайних дверей

Конструкція	Умови використання	Звукоізоляція (дБ) на частотах, Гц					
		125	250	500	1000	2000	4000
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Щитові двері, облицювання фанерою з двох сторін	без прокладки	21	23	24	24	24	23
	з прокладкою із пористою резиною	27	27	32	35	34	35
Типова	без прокладки	13	23	31	33	34	36
Двері П-327	з прокладкою із пористою резиною	29	30	31	33	34	41

Для підвищення звукоізолюючої можливості дверей потрібно ліквідувати щілини між підлогою та дверима за допомогою ущільнюючих прокладок.

А у приміщеннях, які потребують найбільшого захисту (кабінеті директора, психолога, бухгалтера та лікаря) встановити двері з підвищеною звукоізоляцією.

Звукоізоляція вікон теж залежить від поверхневої щільності скла і відсутності утворів. Так як у лабораторії встановлені вікна з однокамерними склопакетами, товщиною 4 мм, та без шумопоглинання теж можемо зробити висновок, що вони не сприяють надійному захисту інформації у приміщенні. Тому рекомендується

встановити вікна подвійного засклення з товщиною повітряного проміжку 4 мм. Проте, зважаючи на те, що лабораторія розташована неподалік від спортивного майданчика слід зробити додаткове облицювання скляного простору звуко поглинальним покриттям.

Перегородки між кабінетами виготовлені з газоблоку. Газоблок має дуже малий індекс шумоізоляції – 43дБ. Тому варто використати такі матеріали як мінеральна та гіпсокартон, щоб забезпечити звукоізоляцію за нормами. Рекомендується встановити звукоізоляцію у кабінетах директора, психолога, бухгалтера та лікаря.

3.3 Висновки

Отже, у зв’язку з розвитком інформаційних технологій правовий захист стає все необхідним. Правовий захист націлений вирішувати такі проблеми:захист персональних даних, захист комерційної таємниці, боротьба з кіберзлочинністю, контроль безпеки інформаційних систем, страхування інформаційних систем. Так як на досліджуваному об’єкті зберігається велика кількість конфіденційних даних, дуже важливо належним чином впровадити правовий захист інформації. Для цього було розроблені політики інформаційної безпеки навчально-наукової лабораторії медико-психологічних досліджень ХНУ та ознайомлено з ними усіх працівників лабораторії. Практичне застосування інженерно-технологічного захисту призведе до зменшення ризику несанкціонованого доступу до конфіденційних даних підприємства. Тому у лабораторії було встановлено 7 камер спостереження у приміщеннях де відбувається обробка інформації, встановлено двері з підвищеною звукоізоляцією у кабінетах які потребують найбільшого захисту, встановлено вікна подвійного засклення з товщиною повітряного проміжку 4 мм та зроблено додаткове облицювання скляного простору звуко поглинальним покриттям, а також встановлено звукоізоляцію у кабінетах директора, психолога, бухгалтера та лікаря.

4 РЕАЛІЗАЦІЯ КОНТРОЛЮ ДОСТУПУ ДО ВЕБСАЙТУ «ЕЛЕКТРОННИЙ ПАСПОРТ ЗДОРОВ'Я СТУДЕНТІВ» НАВЧАЛЬНО-НАУКОВОЇ ЛАБОРАТОРІЇ МЕДИКО-ПСИХОЛОГІЧНИХ ДОСЛІДЖЕНЬ ХНУ

4.1 Дослідження та аналіз вразливостей вебсайту «Електронний паспорт здоров'я студентів»

З кожним днем кількість вебдодатків збільшується, при цьому HTTP і HTTPS трафік є основним джерелом поширення загроз інформаційної безпеки. Неконтрольований доступ в Інтернеті призводить до проникнення вірусів до мережі, сприяє втраті або викраденню конфіденційної інформації, а також впливає на ефективність роботи працівників. Такі інциденти як «взломи» паролів, наслідками яких є витік персональних даних, розголошення конфіденційної інформації частіше всього відбувається через вебресурси.

Сучасні вебзагрози небезпечні для мереж будь якого масштабу. Поширення соціальних мереж, тенденції до зараження легітимних сайтів, різноманітність шкідливого коду примушують приділяти особливу увагу безпеці та застосовувати нові способи контролю доступу [23].

Джерелами загроз можуть бути як зовнішні так і внутрішні загрози, а саме співробітники об'єктів. Керівники компаній мають розуміти, що працівники можуть не лише виконувати службові обов'язки, але можуть сприяти таким ризикам як:

- витік комерційної таємниці через вебканали;
- затримки у роботі вебдодатків чи комунікацій через перевантаження каналів;
- збір в роботі через зараження вірусами від неперевірених та небезпечних сайтів.

Щоб контроль доступу був завжди актуальним та ефективним потрібен постійний аналіз вебресурсів.

Контроль доступу в Інтернет має включати:

- захист вебтрафіку від вірусів;
- керування доступом співробітників до вебдодатків, вебсайтів;
- захист користувачів від переходів за шкідливими посиланнями;
- контроль використання хмарних сервісів;
- запобігання витоку конфіденційних даних;
- відображення статистики використання трафіку організації;
- регулювання завантаженості каналів мережі.

Було проведено перевірку вебсайту «Електронний паспорт здоров'я студентів» та було виявлено ряд вразливостей.

Відсутність перевірки вхідних даних. Будь який сайт має перевіряти вхідні дані, та виявляти дані які можуть нести загрозу. В наш час не можна довіряти тому, що ми отримуємо від користувача, адже є багато бажаючих які вирішили перевірити на стійкість вашу систему захисту інформації, вже не кажучи про конкурентів, які намагатимуться будь-яким способом отримати потрібну інформацію. Потрібно завжди перевіряти дані на стороні сервера, навіть якщо наявні перевірки на стороні клієнта, тому що зловмисник може відключити JavaScript, або ж зовсім не використовувати браузер. В нашому випадку перевірки не було ні на стороні клієнта, ні на стороні сервера.

Відсутній захист від XSS атак. XSS атака – це атака, заснована на під'єднанні клієнтського коду у вразливі сторінки сайту. Наприклад, на сайті є форма яка дозволяє вводити власний варіант відповіді і ці дані потім виводяться на сторінці де зберігаються відповіді робітника на конкретний тест. Якщо якийсь користувач введе в форму код JavaScript, який не буде відфільтрований, то цей код буде інтерпретований браузером. А це може призвести як до простого редиректу користувачів на стороні URL, так і до цілих DoS-атак спричинених такими редиректами.

Було здійснено перевірку нашого вебсайту на захист від атак такого типу.

У текстове поле введено JavaScript код з перенаправленням за покликанням https://google.com (рис. 4.1)

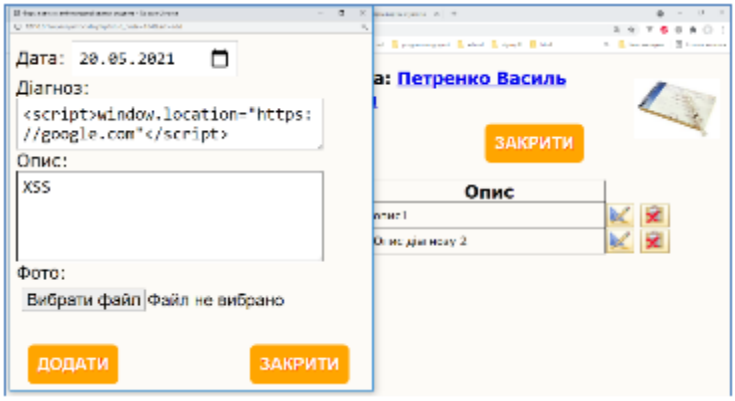


Рисунок 4.1 – Додавання коду JavaScript у поле форми

Після виконання передачі даних на сервер та їх збереження у БД отримаємо результат представлений на рис. 4.2

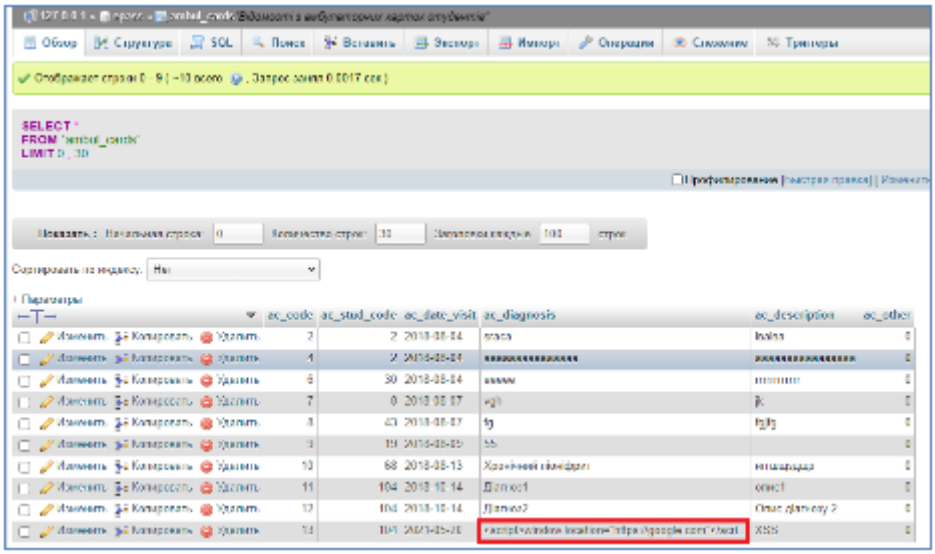


Рисунок 4.2 – Результат збереження коду JS у БД

В результаті маємо збереження JavaScript коду у БД, і його автоматичне виведення разом з іншими даними на вебсторінці, а отже і виконання на стороні клієнта. Даний приклад відображає вразливість XSS-атак.

– відсутній захист від CSRF атак, зловмисники часто використовують вразливості в коді, для того щоб виконати якісь дії без відома самого користувача. Такі атаки спрацьовують у випадках, коли логіка сайту спроектована не правильно,

а саме обробка GET-запитів. Тобто ніякі дані не повинні змінюватись у відповідь на GET-запити. Під час перевірки сайту до цього виду атак, ми змоделювали ситуацію, для цього використано такий код

Button

Це призвело до того що GET-запит виконався і ми змогли подивитися результати тестування іншого користувача.

– відсутній захист від SQL-ін'єкцій. SQL-ін'єкція це вид атаки, коли зловмисник вводить команди SQL в поле вводу (input, textarea, параметри _GET/_POST, cookies і тд.) на вебсторінці. Навіть методом «Сліпих» ін'єкцій вдалось довести вразливість сайту до атаки цього виду.

Під час перевірки вебсайту було змодельовано SQL атаки.

Для прикладу розглянемо SQL-ін'єкцію під час передавання числових даних методом GET, після числового значення параметру поставимо апостроф (рис. 4.3)

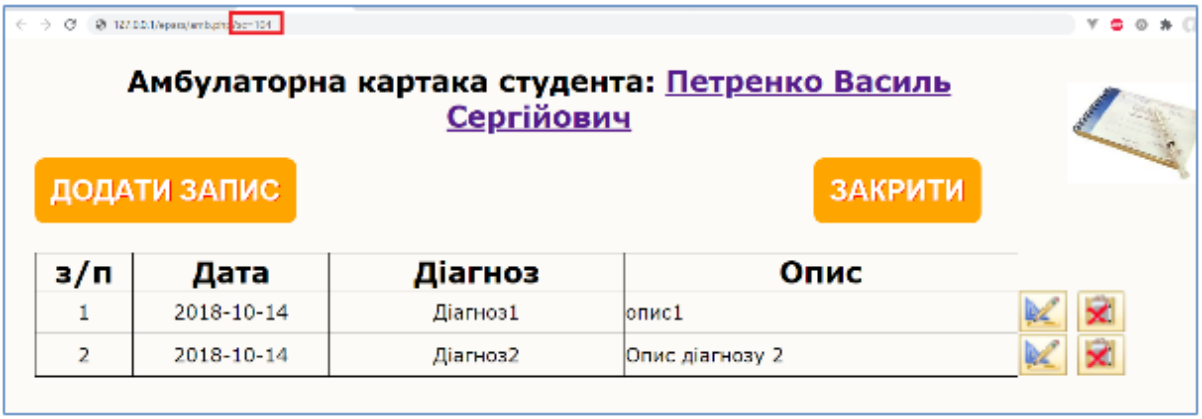


Рисунок 4.3 – Перевірка на присутність SQL-ін'єкції для числового значення параметра

У результаті отримаємо помилки, що свідчить наявність SQL-ін'єкції (рис. 4.4)

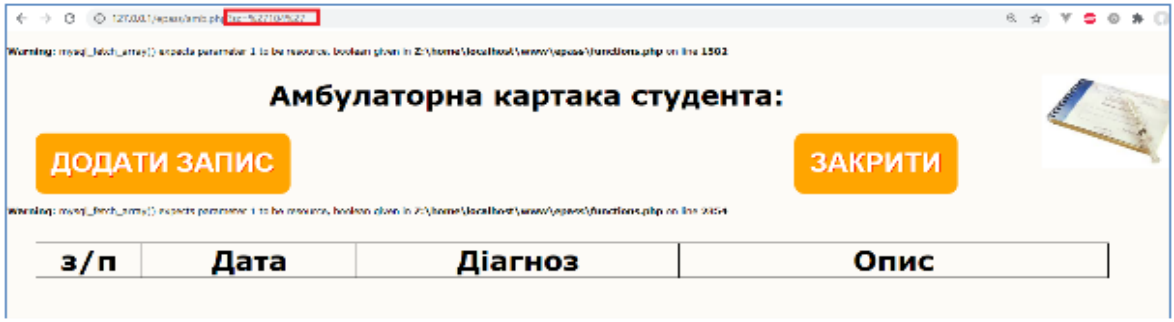


Рисунок 4.4 – Підтвердження наявності SQL-ін’єкції для числового параметра

Таким чином ми маємо можливість виконати запит з в якому об’єднаємо за допомогою оператора UNION ще один запит, потрібно провести ряд досліджень на кількість полів (UNION SELECT 1, 2 , …), їх назви, та отримати всі об’єднані дані з даної таблиці. Для прискорення підбору кількості полів у запиті можна використати операцію групування GROUP BY, наприклад, якщо запит: index.php?id=1 GROUP BY 3 не повертає помилку, це означає, що полів більш ніж 3, і якщо при значенні GROUP BY 5 повернуто помилку – це свідчить, що полів 4.

Для відкидання результату першого запиту достатньо підібрати значення неіснуючого ID, для прикладу, id=-1. Для виведення шуканої інформації потрібно замінити цифри у другому запиті на назви полів, а шуканий запит відібрати за ID, index.php?id=-1 UNION SELECT name, 2, password, 4 FROM users WHERE id=1.

Для рядкового типу також виявлено вразливість (рис. 4.5)

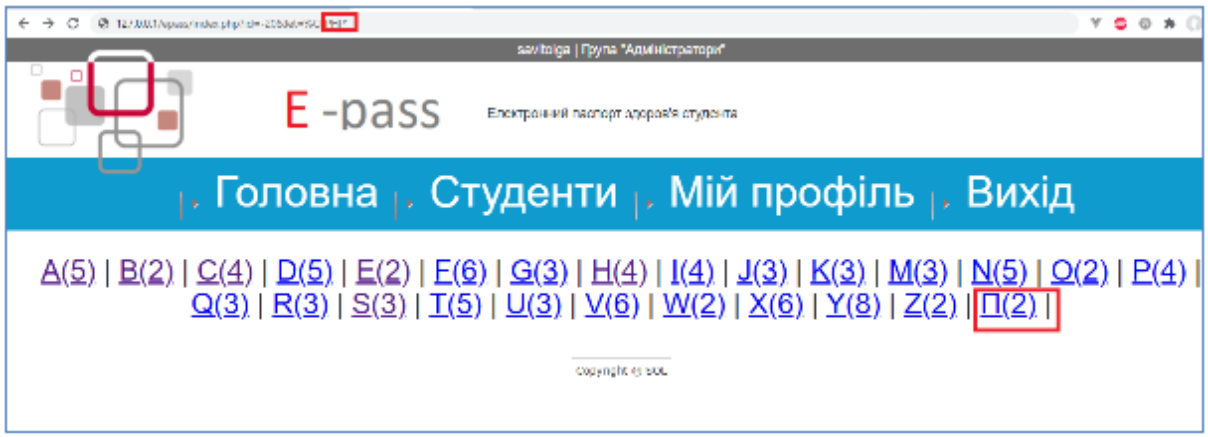


Рисунок 4.5 – Перевірка вразливості SQL-ін’єкції для рядкового параметру

Підтвердження видно з рис. 4.6

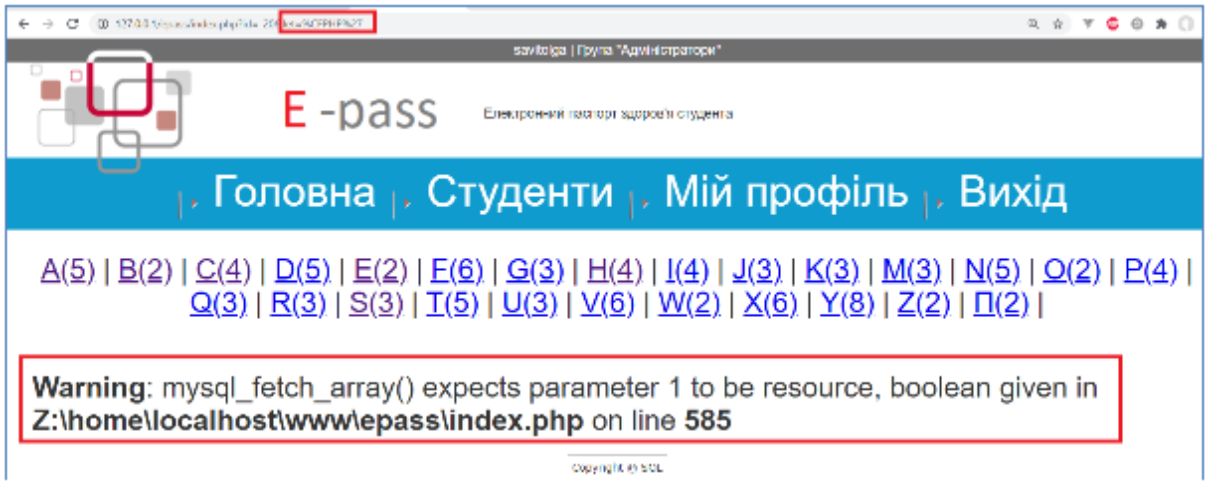


Рисунок 4.6 - Підтвердження наявності SQL-ін’єкції для рядкового параметру

У випадку із рядковою величиною потрібно додати апостроф на початку та знак коментаря в кінці.

Наприклад, якщо підібрати кількість полів та визначити їх назви:

index.php?id=-20&let=%CF’ UNION SELECT 1, name, 2, 3 FROM users WHERE id=1 --

Для вдалого виконання оператора об’єднання UNION необхідно, щоб структури запитів, що об’єднуються були однакові. Досягнувши цього, наприклад, підбором та аналізом помилок виконання запитів, можна отримати довільні дані з таблиці, навіть ті, які не передбачалося оприлюднювати. Якщо пароль у БД зберігався в вихідному стані, не зашифрований, тоді задача доступу до решти даних БД стає набагато простішою, визначивши адміністратора і отримавши доступ, наприклад, до адмін панелі.

– Відсутність захисту файлової системи.

На рис. 4.7 – Приклад коду використаного для файлової системи зображено код, який був використаний для файлової системи. Такий підхід дає доступ до частини файлової системи сервера, а може навіть і до конфігураційних файлів PHP.

Рисунок 4.7 – Приклад коду використаного для файлової системи

– Відсутність захисту даних сесії, дані сесій досліджуваного сайту зберігаються на shared-хостингу і є не зашифрованими, це означає, що при певних обставинах доступ до файлів сесії користувачів без проблем може отримати будь-який інший користувач цього хостингу.

– Відсутність обробки помилок і виключень обробка помилок. На вебсайті для обробки помилок не використовуються механізми виключень, тобто створення ієрархій виключень на основі класу Exception і коректної їх обробки в блоках try...catch. Замість того помилки видно користувачам, а це може стати гарною точкою пошуку вразливостей для зловмисників.

– Відсутність захисту файлів що підключаються. PHP- сценарії часто включають в себе інші сценарії, використовуючи інструкції include і require. Розробники сайту закінчували імена таких файлів на суфікс ‘.inc’, це є небезпечно тим що вебсервер може бути налаштований таким чином, що не буде використовувати .inc-файли в якості PHP-сценаріїв, а замість цього буде віддавати їх як text-plain. Таким чином будь-хто зможе отримати доступ до вихідного коду сайту, або ж до файлів конфігурації з логінами/паролями підключеними до БД.

– Відсутність захисту від DDoS-атак. Атаки типу DDoS – це спроби завдати шкоди, зробивши недоступною систему, наприклад вебсайт. Зазвичай зловмисники генерують велику кількість пакетів чи запитів, які перегружають роботу системи. Наприклад, відсутність перевірки «я не робот» дає можливість відправляти безліч запитів на сервер, що за певних умов може призвести до перевантаження та поломки сервера.

– Відсутність Backup. Іноді трапляються апаратні збої, якщо не робити Backup то дані можуть зникнути без можливості повернення.

– Відсутність використання PDO.

– Використання старої версії PHP.

4.2 Реалізація захисту та контролю доступу до вебсайту «Електронний паспорт здоров’я студентів»

Рекомендації щодо програмного та технічного напрямку.

Взаємодія з БД, захищаємо дані.

Насамперед, для впровадження надійного захисту та коректного функціонування вебсайту було здійснено перехід на нову версію PHP.

Це обумовлено тим, що з кожним оновленням додаються нові можливості, а також покращується захист від кібератак. Наприклад з’явився інтерфейс SessionHandlerInterface, впровадили використання PDO і багато іншого.

В PHP є можливість взаємодіяти з базами даних засобами mysql, mysqli і PDO. Mysql повністю перестав підтримуватися у PHP 7, але його аналогом виступає mysqli, що дозволяє застосовувати функціональний та об’єктно-орієнтований підхід у програмуванні. PDO – PHP Data Objects, розглядається тільки об’єктно-орієнтований підхід, що призводить до написання універсального коду, який зручний для тестування, повторного використання та масштабування в межах вебдодатків масового та корпоративного рівнів.

Якщо проєкт був написаний із використанням MySQL і з’являється потреба перейти на PostgreSQL, тоді що найменше потрібно замінити всі mysqli_connect() на pg_connect() ті всі аналогічні функції для роботи із запитами та даними. Але у випадку з PDO достатньо змінити тільки декілька параметрів у файлах конфігурації.

Зв’язаність параметрів

Якщо використовувати зв’язуванні параметри, отримуємо гнучкість складання запитів та покращуємо захист від SQL-ін’єкцій.

Докладніше про PDO

Для встановлення підключення до БД потрібно створити новий об’єкт PDO та передати йому ім’я джерела даних, називають DSN. В загальному, DSN складається з назви драйверу та рядку підключення, що розділяються двокрапкою.

На відміну від mysqli в PDO є два типи запитів: ті що повертають результат (show, select) та відповідно ті що його не повертають (delete, insert, ...).

Підготовлені запити та зв’язні параметри

Під час виклику $obj->query(), де $obj = $connection, а $connection – об’єкт встановлення з’єднання з БД, наприклад, $connection = new PDO('mysql:host = localhost; dbname = base; charset = utf8', 'root', 'pas'), утворюється підготовлений запит. Підготовлений запит – це спроможність системи керування базами даних отримати шаблон запиту, відкомпілювати його та виконати після отримання значень змінних, що використовуватися у шаблоні. Схожим чином працюють шаблонізатори Smarty, Blade, Twig.

Приклад використання підготовленого запиту PHP, PDO

$s = $connection -> prepeare(‘SELECT * FROM users WGERE id = :id’);

В даному коді підготовлений запит на вибірку з полем ID рівним значенню, яке буде використано замість :id. СКБД проаналізує і відкомпілює запит, також можливе й кешування. Далі потрібно передати параметр та виконати запит:

$param = 3;

$s -> execute([‘id’ => $param]);

Також отримати дані:

$res = $s -> fetchAll(PDO::FETCH_ASSOC);

Переваги використання зв’язаних параметрів

PDO надає зручні можливості екранування користувацьких даних. Під час виклику методу prepare(), СКБД виконує аналіз та компіляцію даних, далі в циклі відбувається тільки вибірка даних з вказаним параметром, такий підхід прискорює отримання даних, відповідно зменшує час на виконання коду додатку.

Використання типізованих зв’язаних параметрів

Наявність вказівки типу параметра підвищує читабельність та зрозумілість коду, обслуговування та спрощує відлагодження коду, прискорює розробку.

Мова PHP розвивається, розробники повинні йти в ногу із розвитком технологій. Використання розширення PDO дозволить писати компактний, зрозумілий та безпечний код.

Дослідивши наявний вебсайт та проаналізувавши всі наявні вразливості, було прийнято рішення переписати його використовуючи сучасний фреймворк мови PHP. Для забезпечення комплексного захисту, який дозволить усунути всі виявленні вразливості було обрано фреймворк Laravel та такий стек технологій: HTML 5, CSS3(sass), Bootstrap, JavaScript, php 7, MySQLI. Такий вибір був зумовлений наявною базою засобів захисту інформації.

Наведемо для прикладу з деякі функції захисту з фреймворку Laravel.

Захист пароля

Laravel надає клас “Hash”, який забезпечує безпечний кеш Bcrypt. Наприклад, $pas = Hash::make('wordsecret');

Функція make приймає значення в якості аргументу і повертає хеш значення. Хешоване значення можна перевірити за допомогою функції check(), таким чином, Hash::check('wordsecret', $pas), дана функція повертає логічне значення true – якщо пароль співпадає і відповідно false – якщо пароль не співпадає.

Аутентифікація користувачів ще одна функція безпеки Laravel. Фреймворк Laravel дозволяє спростити аутентифікацію, для цього можна використати метод Auth::attempt. Для прикладу:

```
if (Auth::attempt(array('email' => $mail, 'password' => $pas))) {
  return Redirect::intended('/');
}
```

Метод Auth::attempt приймає в якості аргументу облікові данні та порівнює їх з обліковими даними у БД, якщо данні співпадають повертає значення true і відповідно у іншому випадку false.

Захист віт CSRF – міжсайтової підробки запитів, та XSS – атак. Атака з використанням крос-сайтового скриптингу здійснюються при умові, що зловмисник має можливість розмістити код JavaScript на боці клієнта на сторінках, які переглядатиме інші користувачі. Для захисту від подібного типу атак, потрібно

завжди перевіряти користуваціькі данні та не допускати додавання небезпечних конструкцій. В шаблонізаторі Blade потрібно використовувати синтаксис подвійної прив'язки ({{$data}}), а таке відображення {!!$data!!} потрібно застосовувати, якщо є впевненість у безпечності даних і їх можна відобразити без додаткової перевірки.

Протистояння SQL-ін'єкціям, закладено у фрейморці за замовчуванням, конструктор запитів і Eloquent використовують клас об'єктів даних PHP (PDO). PDO використовує підготовлені оператори, які дозволяють безпечно передавати довільні параметри без необхідності їх видалення та санації.

Cookies – безпечні за замовчуванням. Фреймворк Laravel дозволяє просто створювати, читати та вимикати файли cookie за допомогою класу Cookie. У фреймворку автоматично всі файли cookie підписано та зашифровано, відповідно, якщо їх підробити, Laravel автоматично їх відкине, а також їх неможливо зчитати на боці клієнта за допомогою JavaScript.

Примусове використання HTTPS під час обміну не публічної (змінні сеансу для реєстрації від імені користувача) інформації автоматично блокує перехват зловмисниками інформації в одній мережі.

Реалізація захисту вебдодатку засобами фреймворка Laravel

Вимоги до БД, а саме стосовно таблиці users. Довжина стовпця пароля не менше 60 символів, найкращий варіант 255, також необхідна наявність поля remember_token також рядкового типу довжиною не менше 100 символів, це поле для збереження токена користувача, якщо вони оберуть опцію «запам'ятати мене» під час входження у додаток (рис. 4.8-4.9).

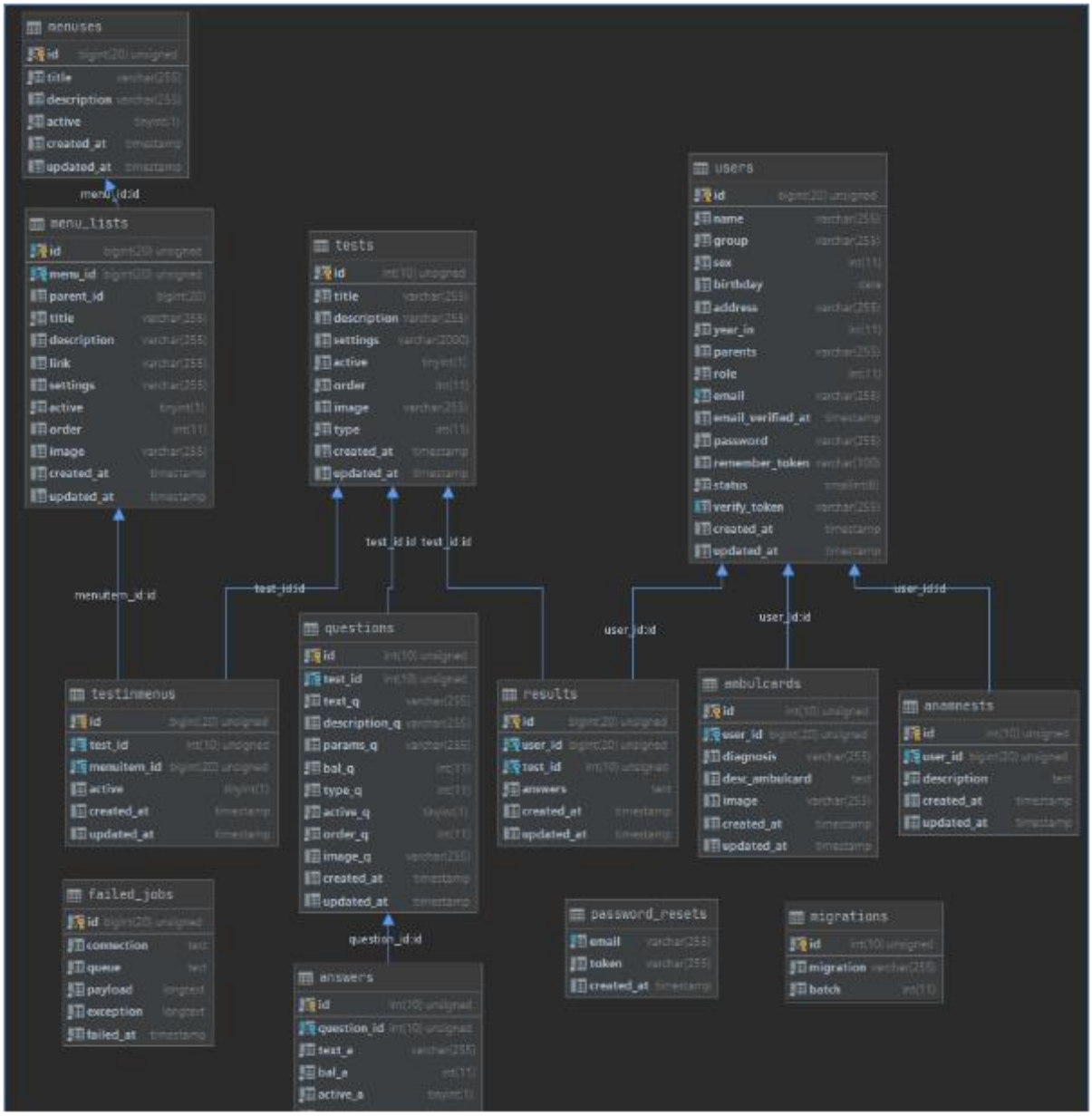


Рисунок 4.8 – «Схема даних вебсайту Epass»

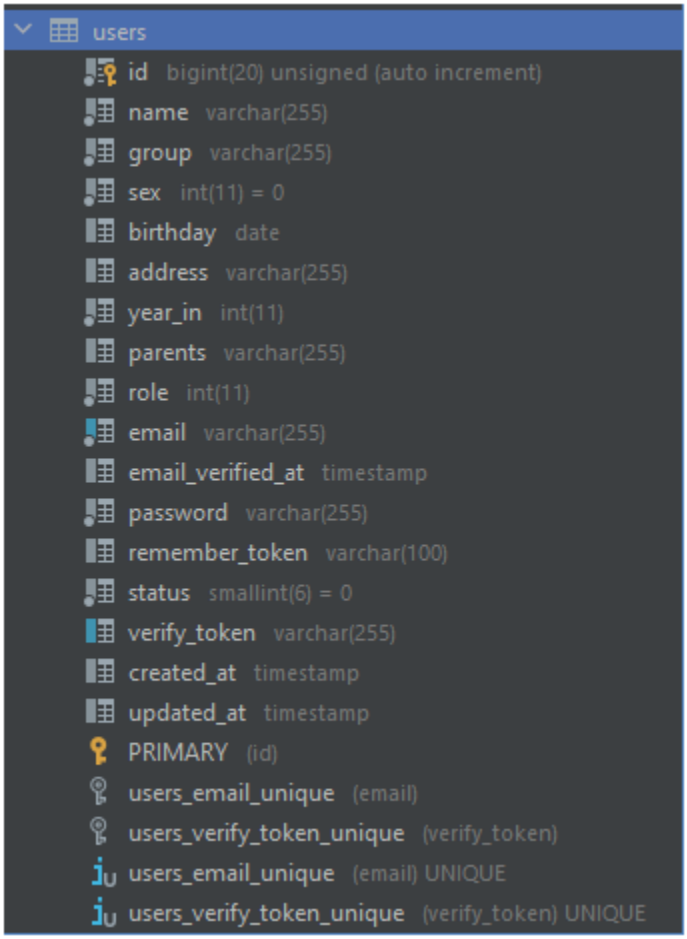


Рисунок 4.9 – «Структура таблиці users, для успішного використання Auth»

Маршрутизація

Laravel містить пакет laravel/ui, який забезпечує швидке формування всіх маршрутів та представлень (шаблонів), що необхідні для аутинтефікації. Після встановлення та виконання даного пакету командами composer require laravel/ui:^2.4, php artisan ui vue – uth буде згенеровані представлення реєстрації та входження в систему, а також маршрути для всіх кінцевих точок аутентифікації. Також буде згенеровано декілька вбудованих контролерів в пространстві імен App\Http\Controllers\Auth: RegisterController, LoginController, ForgotPasswordController. Кожен контролер використовує трейт для використання власних методів. («Згенеровані контролери для аутентифікації» та «Згенеровані представлення для аутинтефікації» відображені на рис. 4.9 -4.10

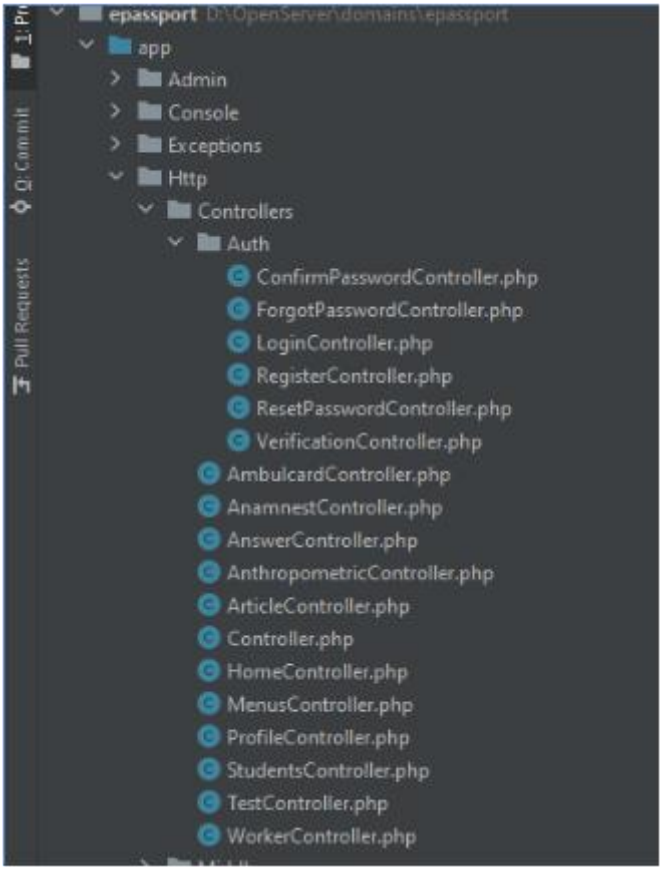


Рисунок 4.9 – Згенеровані контролери для аутентифікації

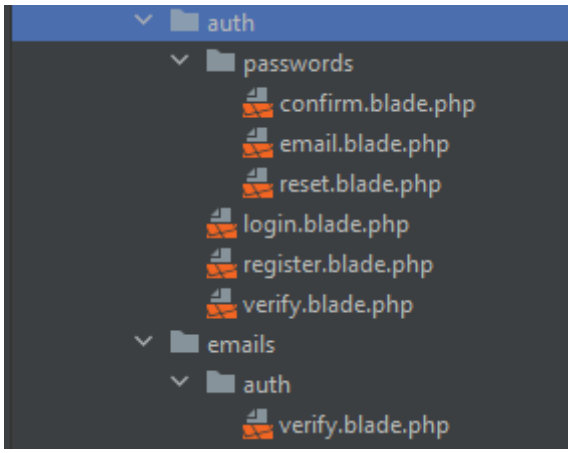


Рисунок 4.10 – Згенеровані представлення для аутентифікації

Лістинги фрагментів шаблонізатора Blade форми реєстрації Додаток A, авторизації Додаток B, перевірки Додаток D, змінення паролю Додаток C, листа з покликанням на змінення пароря Додаток E та підтвердженням пароля Додаток F.

Також слід відмітити наявність @csrf – захист від CSRF (Cross-Site Request Forgery). На формах присутні блоки виведення помилок валідації даних та повернення «старих» даних, що були введені до відправки на сервер, це зручно для користувача, немає потреби постійно заповняти поля, зрозуміло не валідні дані доведеться змінити. Також присутня кнопка нагадування пароля, через надсилання листа з посиланням на роут змінення пароля, також лист містить токен, який буде автоматично звірено після переходу на відповідний роут.

Фрагменти листингів контролерів аутентифікації в Laravel

Додаток G «Фрагмент лістингу LoginController»

В даному фрагменті коду під час побудови екземпляру класу LoginController, який наслідує базовий клас Controller «class LoginController extends Controller» застосовується «посередник» middleware для перенаправлення на вихід з сеансу. Метод authenticate з параметрами типу Request та User визначає чи активовано обліковий запис даного користувача. У випадку неактивованого перенаправлення на входження і передавання повідомлення про необхідність підтвердження свого облікового запису через електронну пошту, а у випадку вірних даних перенаправлення на головну сторінку.

Додаток F «Фрагмент лістингу коду RegisterController»

Даний контролер містить функцію валідації даних, аргумент типу масив, і повертає результат типу масив. Метод register з параметром Request, метод перевіряє чи успішна валідація і у випадку успіху, відбувається подія створення облікового запису користувача, дані якого були у Request. Далі перенаправлення на сторінку з повідомленням перевірки пошти, на яку надіслано листа з покликанням на активацію облікового запису, покликання перенаправить на даний контролер з застосуванням методу ferify з параметром $token, даний метод перевірить відповідність токена і у випадку успішної перевірки змінить статус даного користувача ідентифікованого за токеном та перенаправить на сторінку з повідомленням успішної активації облікового запису.

Був розроблений контроль доступу до вебсайту.

Всі запити http були розподілені на неавторизованих та авторизованих користувачів.

Не авторизовані користувачі можуть лише переглядати довідкову інформацію (головну сторінку, сторінку новин, статей), авторизовані користувачі поділяються за ролями:

- Суперадмін – має усі права сайту. Може повністю керувати вебсайтом, а саме додавати користувачів чи видаляти, може змінювати контент сайту, має доступ до адміністративної панелі, може змінювати дані користувачів, додавати чи видаляти тести і багато іншого.
- Адмін – має право на адміністративну панель. Може авторизовувати користувачів, змінювати контент сайту.
- Викладач – має право на додавати тести та має доступ до результатів та аналітики по власних тестах
- Лікар – має право додавати тести та переглядати результати та аналітику усіх тестів
- Студент – має право на доступні тести в режимі проходження та перегляд власних результатів без підсумків

Також для захисту вебсайту від кібератак здійснені такі заходи:

- всі форми містить CSRF токен для контролю джерела відправки даних;
- кожен запит проходить підготовку PDO, яка вбудована в Laravel;
- у всіх контролерах здійснюється перевірка періодичності запитів для блокування DDoS атак;
- шифрування паролю в Laravel. Laravel використовує OpenSSL для шифрування AES-256 і AES-128. Він також підтримує безпеку MAC - message authentication code, що гарантує, що дані не будуть змінені після шифрування;
- на всіх формах здійснено валідацію даних на клієнтській та на серверній стороні. На клієнтській стороні це здійснено за допомогою HTML, JavaScript, а на стороні сервера за допомогою стандартного валідатора Laravel.

4.3 Реалізація алгоритмів по визначенню початку атаки і виділенню шкідливого трафіку та захист вебсайту від DDoS-атак

DDoS-атака - розподілена атака, спрямована на відмову в обслуговуванні. В результаті атаки такого типу мережевий ресурс, що атакується, отримує лавиноподібну кількість запитів, які не встигає обробити сервер. Існує міф що атаки типу DDoS здійснють тільки на популярні сайти, проте останнім часом стрімко зросла кількість актак до «середніх» та «невеликих» сайтів. Така тенденція спричинена і зміною мотивів зловмисників. Раніше причиною виникнення DDoS-атак були протести, хуліганство і т.д., а сьогодні все частіше метою є завдання шкоди конкуренту, вимагання або терористичні операції.

Аналіз засобів протидії показав, що в даний час більший розвиток отримала група засобів протидії, призначена для відбиття потужних атак. До цих засобів входять, як правило, дорогі засоби, що призначені для великих провайдерів або компаній. Засоби протидії невеликим і середнім атакам, що розміщенні на сервері, представлені в незначній кількості. При цьому аналіз вхідного трафіку на рівні додатків може бути більш ефективним. З одного боку, проведення такого аналізу економічно менш затратно, з іншого – може бути цілком достатнім для відбиття малих і середніх атак, тенденція домінування яких вже намітилася.

Для захисту лабораторії пропонується впровадження розробленого алгоритму виявлення DDoS-атак і шкідливого трафіку. Алгоритм полягає в виявленні на ранніх стадіях точки початку розподіленої атаки, спрямованої на відмову в обслуговуванні.

На рис. 4.11 показані принципові схеми алгоритмів по визначенню початку атаки і виділенню шкідливого трафіку. Перша схема (рис. 4.11 а), пояснює алгоритм виділення шкідливого трафіку, друга (рис. 4.11 б) і третя (рис. 4.11 в) алгоритми визначення початку атаки.

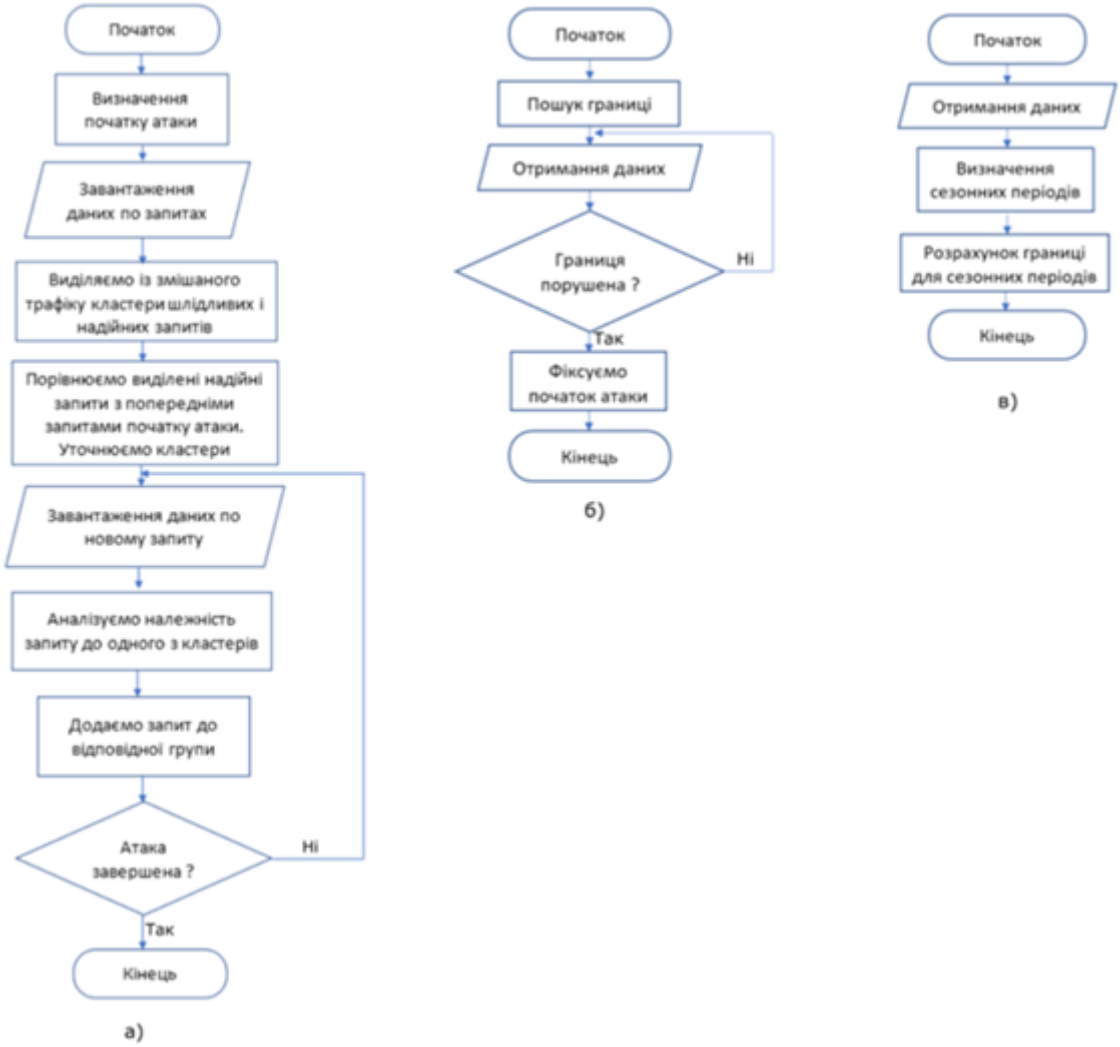


Рисунок 4.11 – Принципові схеми алгоритмів по визначенню початку атаки і виділенню шкідливого трафіку

Спочатку відбувається виклик підпрограм по виявленню сезонних періодів, розпочинається розрахунок для них допустимої межі кількості запитів і визначення початку атаки. Якщо атака почалась, алгоритм повинен розподілити змішаний трафік на два кластери, один з яких містить шкідливі запити, а інший надійні запити. Нові запити аналізуються на приналежність до кластеру і за результатом додаються до відповідного кластеру.

Алгоритм враховує сезонні відхилення в навантаженні, це дає можливість виявляти точку початку атаки на ранніх стадіях і з більшою точністю. Також

додатково проведено дослідження, спрямоване на підтвердження існування сезонності і виявлення типових сезонних періодів.

У лабораторії використовується бездротове з'єднання. А саме Wi-Fi роутери для доступу до Інтернету, проте часто Wi-Fi роутери можуть використати зловмисники для здійснення шахрайських дій.

Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження.

Ефективна система безпеки:

– Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі з будь-якого місця та бути впевненими у захисті передачі інформації.

– Стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.

– Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи.

– Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та партнери можуть бути впевненими у надійному захисті їхньої інформації.

Фрагмент топології мережі лабораторії представлено на рис. 4.12

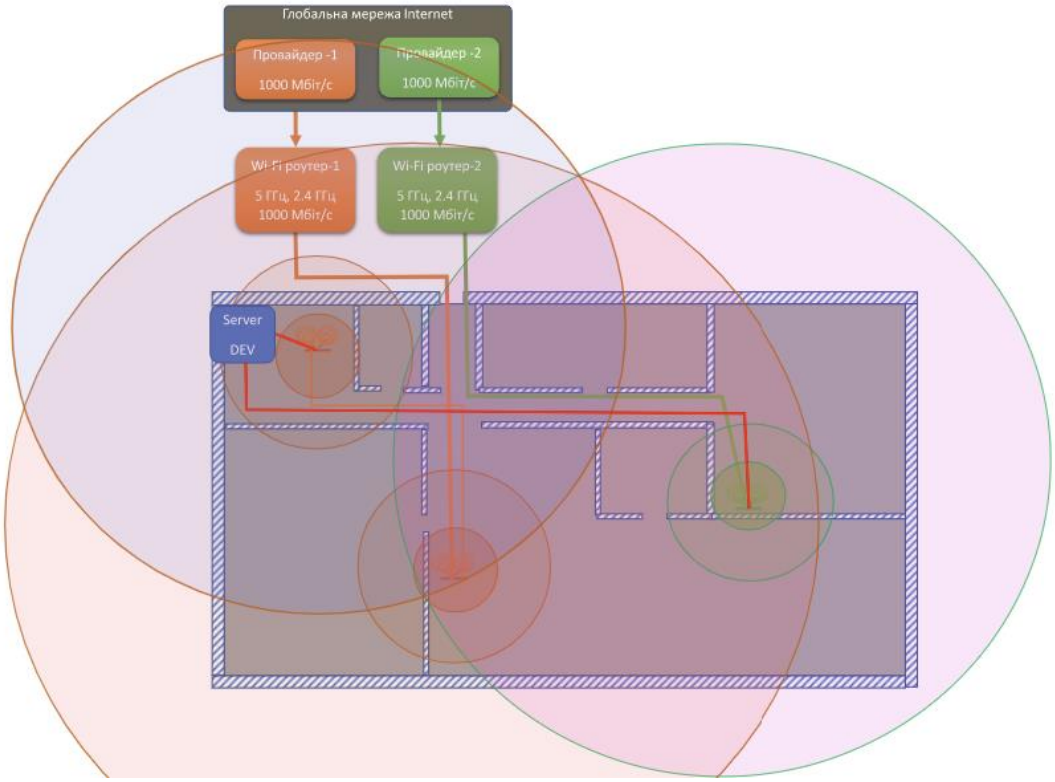


Рисунок 4.12 – Фрагмент топології мережі лабораторії

З рис. 4.12 видно, що мережа не містить багато дротових з’єднань, що значно здешевлює монтаж таких мереж, але з іншого боку послаблюється захист мережі зовні. Тому не менш важливим є захист бездротових з’єднань.

Для зменшення уразливості мережі було впроваджено:

– використання безпечних WiFi-маршрутизаторів бізнес-класу, який містить розширенні можливості конфігурації та пропускної спроможності декількох SSID та інші;

– обмеження доступу до маршрутизаторів, це очевидно, але деякі компанії залишають фізичний доступ до пристроїв всім співробітникам, а іноді і гостям – відвідувачам компанії;

– слідкування за оновленнями програмного забезпечення, які часто слугують виправленню уражень маршрутизаторів;

– використання WPA2 або WPA2 enterprise, що дозволить встановлювати індивідуальні логіни та паролі користувачів ваших WiFi;

− відключення можливість віддаленого адміністрування ваших маршрутизаторів, так як у випадку проникнення зловмисники можуть скористатися зовні і отримати повний доступ до всієї мережі лабораторії;

− налаштування приватного доступу співробітникам та публічний доступ для гостей, таким чином всю мережу буде поділено на дві точки, одна з них буде добре захищена і доступ будуть мати тільки співробітники лабораторії, в той ж час гості – клієнти, партнери, постачальники зможуть отримати доступ до глобальної мережі;

− регулярний моніторинг точки доступу мережі, особливо сусідні точки доступу, які можуть дозволити співробітникам з'єднатися та свідомо або ненавмисно стати джерелом витоку інформації;

− використання VPN підключення, що дасть декілька додаткових функцій безпеки бездротового з'єднання, одна з найважливіших це захист WiFi мережі за межами зони контролю;

− використання оригінального імені мережі та складного паролю;

− контроль трафіку мережі, а саме весь вхідний та вихідний трафік спрямувати через спеціальний проксі-сервер де застосовані політики для різних груп користувачів із прив'язкою до Mac-адрес та IP-адрес. Це здійснено за допомогою ОС FreeBSD та Squid. Розроблений варіант зображено на рис. 4.13.

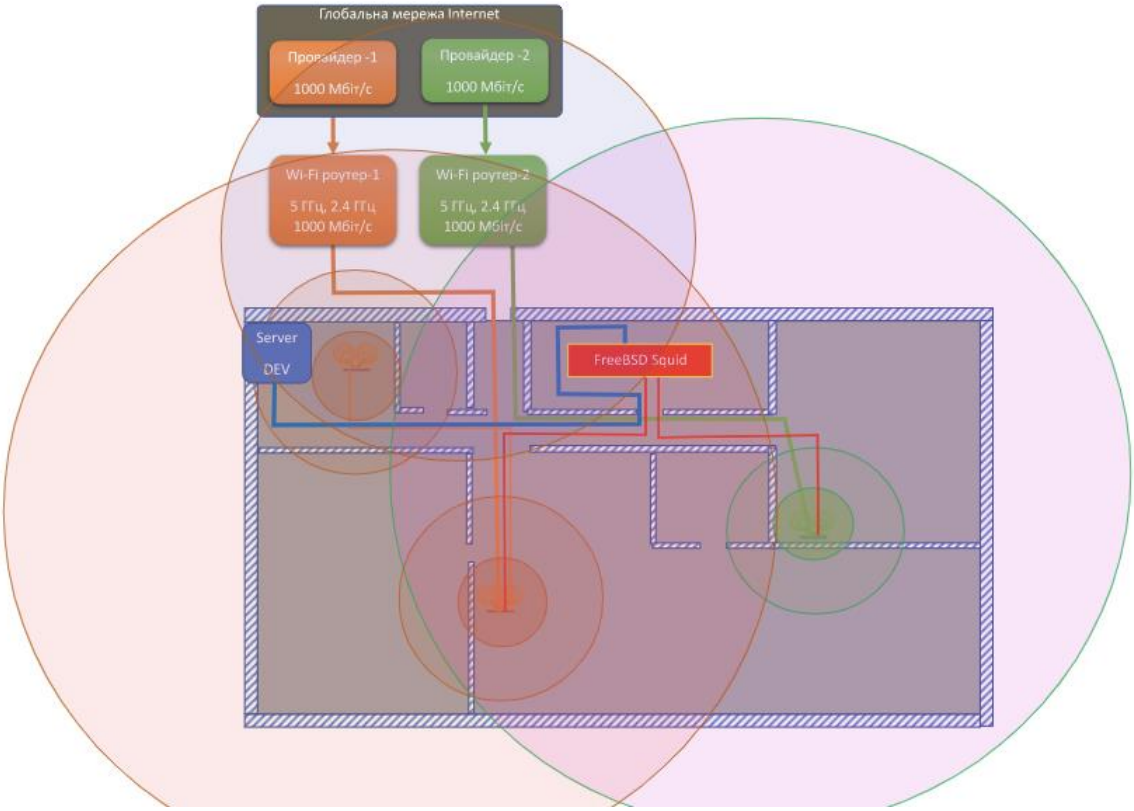


Рисунок 4.13 – Топологія фільтрації трафіку мережі

4.4 Висновки

Отже, під час проведення аналізу вразливостей вебсайту «Електронний паспорт здоров'я студентів» було змодельовано атаки на вебсайт та виявлено ряд вразливостей, таких як незахищеність від SQL-ін'єкцій, відсутність захисту від XSS та CSRF атак, відсутність перевірки вхідних даних, відсутній захист від DDoS-атак та інші. Для реалізації захисту та контролю доступу до вебсайту було модифіковано наявний вебсайт на основі фреймворку Laravel, розширено функціональну можливість вебсайту, впроваджено перевірку вхідних даних як на стороні користувача так і на стороні сервера, впроваджено захист від XSS, CSRF та SQL атак, реалізовано контроль доступу до вебсайту, встановлено антивірусне забезпечення eset business security, для фільтрації трафіку було встановлено VipNet Office Firewall фаєрвол, для виявлення різних атак запропоновано використати Honeypot Manager. Також було розроблено алгоритм визначення початку DDoS атак.

ВИСНОВКИ

Інформаційна безпека передбачає забезпечення захисту даних від розкрадань або змін як випадкового, так і навмисного характеру. Система забезпечення інформаційної безпеки організації – ефективний інструмент захисту інтересів власників і користувачів інформації.

Слід зазначити, що збиток може бути завдано не тільки несанкціонованим доступом до інформації. Він може бути отриманий і в результаті поломки комунікаційного або інформаційного обладнання.

Термін «безпека інформації» описує ситуацію, яка виключає доступ для перегляду, модерації і знищення даних суб'єктами без наявності відповідних прав. Це поняття включає забезпечення захисту від витоку і крадіжки інформації за допомогою сучасних технологій та інноваційних пристроїв.

На даний момент з'являються все нові і нові віруси. На кожен вірус розробляється нове захисне ПЗ або вдосконалюється вже наявне.

Саме тому, захист інформації повинен здійснюватися в сукупності по всіх напрямках. І чим більше прийомів і технологій буде задіяно, тим менше ймовірність виникнення загроз і витоку, тим стійкіше положення компанії на ринку.

Отже, щоб забезпечити захищеність підприємства та досягти цілей бізнесу, потрібно вчасно виявити та не допустити зовнішні і внутрішні загрози.

Під час написання кваліфікаційної роботи проведено:

- дослідження та опис Навчально-наукової лабораторії медико-психологічних досліджень ХНУ;
- дослідження каналів витоку інформації;
- дослідження методів та засобів захисту від вебатак;
- аудит інформаційної безпеки Навчально-наукової лабораторії медико-психологічних досліджень ХНУ;
- аналіз системи захисту інформації лабораторії;
- аналіз виявлення вразливостей та загроз наявних на об'єкті захисту;

− оцінку звукоізоляції приміщення та розроблено заходи для покращення самоізоляції;

− аналіз вразливостей вебсайту;

− моделювання можливих кібер-атак на існуючий вебсайт;

− дослідження контролю доступу до вебсайту.

Результатом кваліфікаційної роботи є:

− розроблено та впроваджено політики інформаційної безпеки навчально-наукової лабораторії медико-психологічних досліджень ХНУ;

− розроблено та впроваджено захист персональної та комерційної інформації шляхом встановлення пожежної сигналізації та відеоспостереження;

− запропоновано встановити шумоізоляцію у кабінеті директора, лікаря та психолога;

− встановлено антивірусне забезпечення eset business security [24];

− розроблено алгоритм визначення початку DDoS атаки;

− впроваджено захист від DDoS атак;

− встановлено контроль за наявними програмами, щоб запобігти;

− встановленню стеганографічного чи криптографічного ПЗ і передачі даних.

Для забезпечення надійного захисту та коректного функціонування вебсайту було здійснено перехід на нову версію PHP. Застосовано функціональний та об’єктно-орієнтований підхід у програмуванні PDO, що дозволяє написання універсального коду, який зручний для тестування, повторного використання та масштабування в межах вебдодатків масового та корпоративного рівнів.

Модифікований наявний вебсайт на основі фреймворку Laravel з використанням таких технологій: HTML 5, CSS3(sass), Bootstrap, JavaScript, php 7, MySQLI. Розширена функціональна можливість вебсайту:

− аутентифікація користувачів з можливістю відновити пароль через пошту;

− налаштовано guards [25]; адміністративна панель на основі Sleeping Owl [26] з такими ролями: адміністратор, користувач, лікар, викладач, студент;

− впроваджено перевірку вхідних даних на стороні користувача за допомогою JavaScript, а також на стороні сервера за допомогою PHP;

- впроваджено захист від XSS, CSRF та SQL атак;
- запропоновано здійснювати обробку помилок та виключень;
- встановлено VipNet Office Firewall фаєрвол, який дозволяє блокувати або пропускати будь-які IP-пакети, що проходять через мережевий адаптер сервера; впроваджено Backup раз в 2 тижні; запропоновано використати Honeypot Manager, для виявлення різних атак з мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. В Україні за рік зафіксували близько мільйона випадків кібератак та кіберзагроз - РНБО [Електронний ресурс] – Режим доступу до ресурса: https://www.ukrinform.ua/rubric-technology/3077451-v-ukraini-za-rik-zafiksuvali-blizko-miljona-vipadkiv-kiberatak-ta-kiberzagroz-rnbo.html

2. Архипов О.Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научнопрактической конференции. – К.: ИПРИ НАН Украины, 2014. – С.18-30.

3. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. / К. Захаренко //Науковий вісник. Серія «Філософія». Харків : ХНПУ. 2017. Вип. 48 (частина І). С. 212–219.

4. Евтеев Д. SQL Injection от А до Я [Електронний ресурс] / Дмитрий Евтеев. – 2008. – Режим доступу до ресурсу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-devteev-AdvancedSQL-Injection.pdf.

5. Melnick J. Top 10 Most Common Types of Cyber Attacks [Електронний ресурс] / Jeff Melnick. – 2018. – Режим доступу до ресурсу: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

6. Защита WEB приложений [Електронний ресурс] / Защита WEB приложений - Режим доступу до ресурсу: https://www.infosec.ru/uslugi/zashchita-web-prilozheniy/

8. Аудит інформаційної безпеки і контроль захищеності [Електронний ресурс]. – Режим доступу: http://www.iso27000.ru/informacionnye-rubriki/auditinformacionnoi-bezopasnosti

9. Концепція технічного захисту інформації в галузі зв'язку України [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua.

10. Дослідження вразливостей Web-сайтів та методів – КПІ [Електронний ресурс] / Режим доступу: http://phone.kpi.ua/wp-content/uploads/2014/06/4.pdf.

11. Доступ до інформації та електронне урядування / Автори- упорядники М. С. Демкова, М. В. Фігель. – К.: Факт, 2004. –336 с.

12. Кримінальний кодекс України//Відомості Верховної РадиУРСР, 1961. – № 2. – С. 14.], цивільний кодекс[Цивільний кодекс України// Офіційний вісник України. – 2003, № 11. – С. 461.]

13. Господарський кодекс України// Відомості Верховної Ради, 2003. – № 11. – С. 462.

14. Конституція України// Відомості Верховної Ради, 1996. – № 30. – С. 141

15. Пашкова В. С. Інформаційна політика і бібліотека // Бібліотека і влада. Збірник статтей до Міжнародної науково-практичної конференції. – К., 2000. – С. 4 - 16.

16. Концепція (основи державної політики) національної безпеки України. Схвалено постановою Верховної Ради України 16.01.1997 // Урядовий кур'єр. – 1997. – 6 лют.

17. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

18. Закон України Про захист персональних даних//Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2297-17#Text

19. Пожежна сигналізація [Електронний ресурс]. 2019 – Режим доступу - http://florian-lviv.com/pozhezhna-syhnalizatsia

20. Хорев, А.А. Технические каналы утечки акустической (речевой) информации. Классификация и характеристика [Текст] / А.А. Хорев // Специальная техника. – 1998. – №1.

21. ДСТУ Б. В. 2.6-85: 2009. Звукоізоляція огороджувальних конструкцій. Методи оцінювання.

22. ДСТУ-Н Б В.1.1-35: 2009. Настанова з проведення розрахунку шуму в приміщеннях і на територіях

23. Дослідження вразливостей Web-сайтів та методів їх ... – КПІ Електроний ресурс: http://phone.kpi.ua/wp-content/uploads/2014/06/4.pdf

24. ESET Endpoint Antivirus для Microsoft Windows [Електронний ресурс] / Режим доступу: https://www.esetnod32.ru/business/products/eea_win/.

25. Аутентификация (Laravel) — Laravel Framework [Електронний ресурс] / Режим доступу: https://laravel.su/docs/5.2/authentication.

26. SleepingOwl Admin Documentation [Електронний ресурс] / Режим доступу: https://sleepingowladmin.ru/#/.

ДОДАТОК А

(Обов’язковий)

Код (лістинг) програмного забезпечення

//… Фрагмент лістингу коду форми авторизації…

```
<form method="POST" action="{{ route('login') }}">
 @csrf
 <div class="form-group row">
 <label for="email" class="col-md-4 col-form-label text-md-right">E-Mail</label>
<div class="col-md-6">
 <input id="email" type="email" class="form-control @error('email') is-invalid @enderror" name="email" value="{{
old('email') }}" required autocomplete="email" autofocus>
 @error('email')
 <span class="invalid-feedback" role="alert">
 <strong>{{ $message }}</strong>
 </span>
 @enderror
 </div>
</div>
<div class="form-group row">
 <label for="password" class="col-md-4 col-form-label text-md-right">Пароль</label>
 <div class="col-md-6">
  <input id="password" type="password" class="form-control @error('password') is-invalid @enderror" name="password"
required autocomplete="current-password">
 @error('password')
 <span class="invalid-feedback" role="alert">
 <strong>{{ $message }}</strong>
 </span>
 @enderror
 </div>
</div>
<div class="form-group row">
 <div class="col-md-6 offset-md-4">
  <div class="form-check">
          <input class="form-check-input" type="checkbox" name="remember" id="remember" {{ old('remember') ? 'checked'
: '' }}>
  <label class="form-check-label" for="remember">
  Запам'ятати
  </label>
          </div>
  </div>
 </div>
  <button type="submit" class="btn btn-primary">
  Увійти
 </button>
 @if (Route::has('password.request'))
 <a class="btn btn-link" href="{{ route('password.request') }}">
  Забули Свій Пароль?
 </a>
 @endif
 </div>
</div>
</form>
...
```

//Фрагмент лістингу коду форми реєстрації

```
<form method="POST"
  action="@if(!Auth::check())
  {{ route('register') }}
  @else
  {{ route('editprofile')}}
  @endif">
  @csrf

…
<div class="form-group row mb-0">
  <div class="col-md-6 offset-md-4">
  <button type="submit" class="btn btn-primary">
        @if(!auth()->check()) Реєстрація @else Змінити @endif
  </button>
  </div>
 </div>
  </form>
 </div>
 </div>
 </div>
 </div>
</div>
…
```

//Фрагмент форми відправки листа для змінення паролю

```
  <div class="card-header">{{ __('Verify Your Email Address') }}</div>

  <div class="card-body">
  @if (session('resent'))
        <div class="alert alert-success" role="alert">
        {{ __('A fresh verification link has been sent to your email address.') }}
  </div>
 @endif

 {{ __('Before proceeding, please check your email for a verification link.') }}
  {{ __('If you did not receive the email') }},
  <form class="d-inline" method="POST" action="{{ route('verification.resend') }}">
  @csrf
  <button type="submit" class="btn btn-link p-0 m-0 align-baseline">{{ __('click here to request another') }}</button>.
 </form>

 …
```

// Фрагмент лістингу коду форми форми змінення пароля

```
…
 <form method="POST" action="{{ route('password.update') }}">
        @csrf

  <input type="hidden" name="token" value="{{ $token }}">

        <div class="form-group row">
        <label for="email" class="col-md-4 col-form-label text-md-right">{{ __('E-Mail Address') }}</label>

        <div class="col-md-6">
        <input id="email" type="email" class="form-control @error('email') is-invalid @enderror" name="email" value="{{
$email ?? old('email') }}" required autocomplete="email" autofocus>

        @error('email')
        <span class="invalid-feedback" role="alert">
        <strong>{{ $message }}</strong>
```

```
            </span>
    @enderror
            </div>
            </div>

            <div class="form-group row">
            <label for="password" class="col-md-4 col-form-label text-md-right">{{ __('Password') }}</label>

            <div class="col-md-6">
            <input id="password" type="password" class="form-control @error('password') is-invalid @enderror"
name="password" required autocomplete="new-password">

            @error('password')
            <span class="invalid-feedback" role="alert">
            <strong>{{ $message }}</strong>
            </span>
            @enderror
            …
   <div class="form-group row mb-0">
            <div class="col-md-6 offset-md-4">
            <button type="submit" class="btn btn-primary">
     {{ __('Reset Password') }}
            </button>
            </div>
            </div>
            </form>
   ...


//Фрагмент лістингу коду листа з покликанням для змінення пароля
…

<div class="card-header">{{ __('Reset Password') }}</div>

  <div class="card-body">
  @if (session('status'))
   <div class="alert alert-success" role="alert">
   {{ session('status') }}
   </div>
  @endif

  <form method="POST" action="{{ route('password.email') }}">
  @csrf

  <div class="form-group row">
  <label for="email" class="col-md-4 col-form-label text-md-right">{{ __('E-Mail Address') }}</label>

  <div class="col-md-6">
   <input id="email" type="email" class="form-control @error('email') is-invalid @enderror" name="email" value="{{
old('email') }}" required autocomplete="email" autofocus>

  @error('email')
   <span class="invalid-feedback" role="alert">
   <strong>{{ $message }}</strong>
   </span>
   @enderror
   </div>
  </div>

  <div class="form-group row mb-0">
   <div class="col-md-6 offset-md-4">
    <button type="submit" class="btn btn-primary">
            {{ __('Send Password Reset Link') }}
            </button>
```

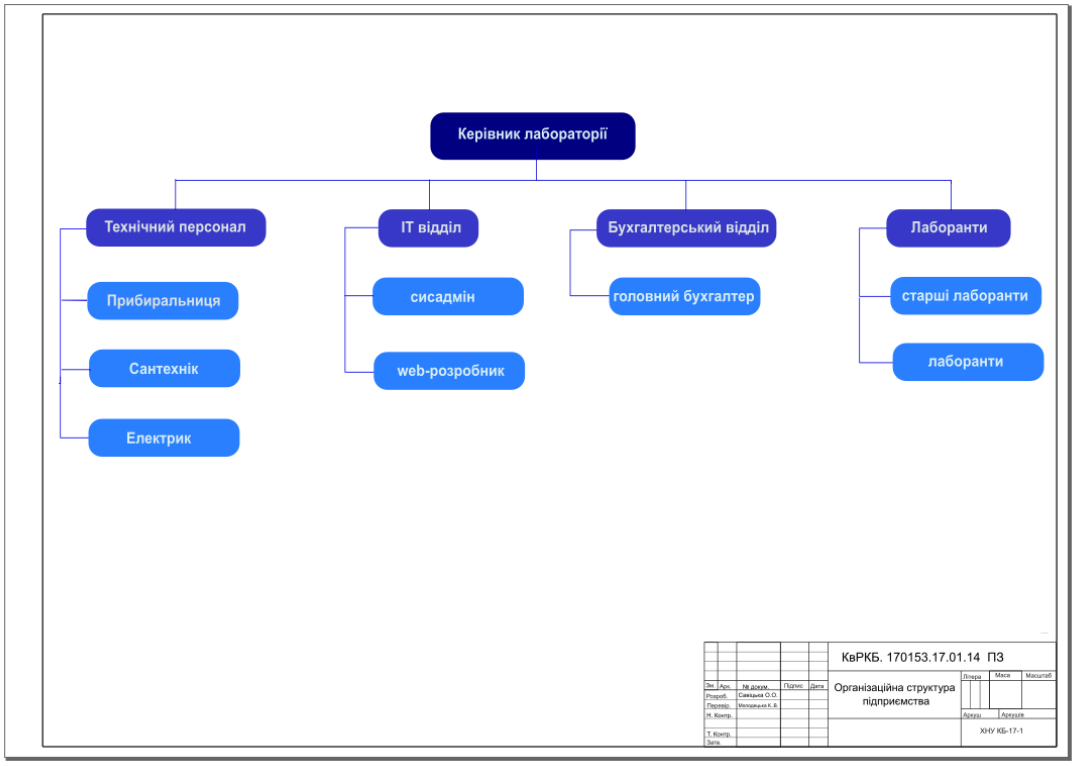
```
 ...
//Фрагмент лістингу коду підтвердження змінення пароля

 …

<div class="card-header">{{ __('Confirm Password') }}</div>

  <div class="card-body">
   {{ __('Please confirm your password before continuing.') }}

   <form method="POST" action="{{ route('password.confirm') }}">
   @csrf

   <div class="form-group row">
            <label for="password" class="col-md-4 col-form-label text-md-right">{{ __('Password') }}</label>

   <div class="col-md-6">
            <input id="password" type="password" class="form-control @error('password') is-invalid @enderror"
name="password" required autocomplete="current-password">

            @error('password')
            <span class="invalid-feedback" role="alert">
            <strong>{{ $message }}</strong>
            </span>
            @enderror
            </div>
   </div>

   <div class="form-group row mb-0">
            <div class="col-md-8 offset-md-4">
            <button type="submit" class="btn btn-primary">
            {{ __('Confirm Password') }}
            </button>

            @if (Route::has('password.request'))
            <a class="btn btn-link" href="{{ route('password.request') }}">
            {{ __('Forgot Your Password?') }}
             </a>
            @endif
            </div>
            </div>
            </form>
   ...
// Фрагмент лістингу LoginController
use AuthenticatesUsers;
 /**
  * Where to redirect users after login.
  *
  * @var string
  */
 protected $redirectTo = '/';

 /**
  * Create a new controller instance.
  *
  * @return void
  */
 public function __construct()
 {
            $this->middleware('guest')->except('logout');
 }

 public function authenticated(Request $request, $user)
```

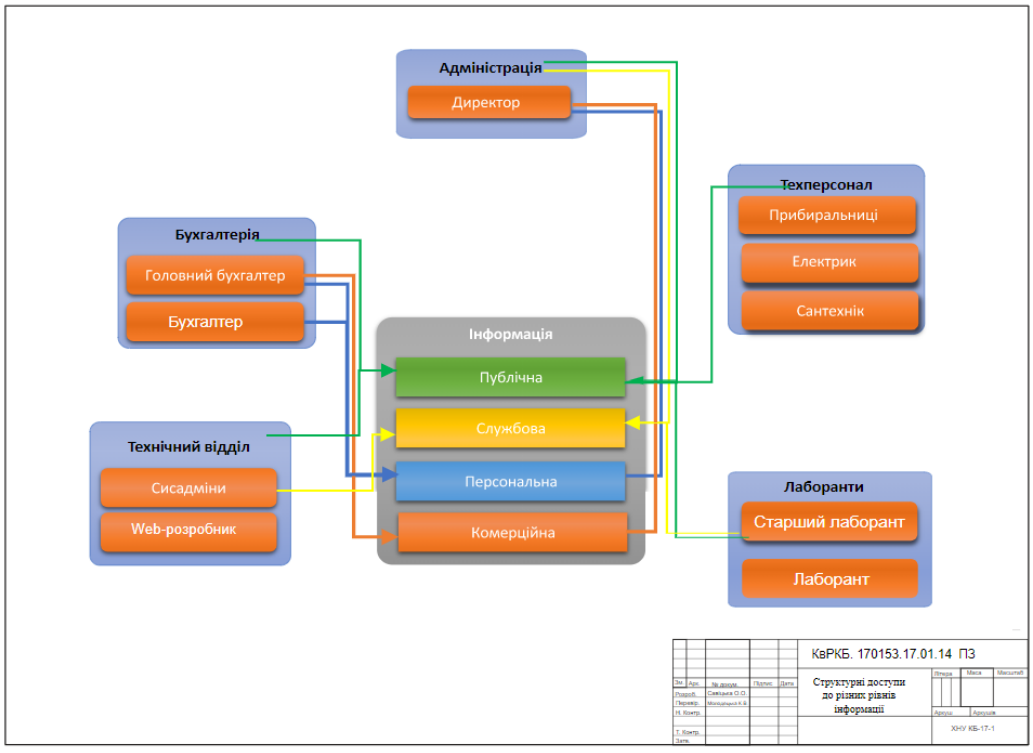
```
{
        if ($user->status != User::STATUS_ACTIVE) {
        $this->guard()->logout();
        return back()->with('error', 'You need to confirm your account. Please check your email.');
    }
        return redirect()->intended($this->redirectPath());
}
// Фрагмент лістингу RegisterController
use RegistersUsers;
protected $redirectTo = '/';
public function __construct(){
        $this->middleware('guest');
}
protected function validator(array $data){
        return Validator::make($data, [
        'name' => ['required', 'string', 'max:255'],
        'email' => ['required', 'string', 'email', 'max:255', 'unique:users'],
        'password' => ['required', 'string', 'min:8', 'confirmed'],
        …
        'role' => [],
        ]);
}

protected function create(array $data){
        $user = User::create([
        'name' => $data['name'],
        'email' => $data['email'],
        'password' => Hash::make($data['password']),
        …
        'verify_token' => Str::random(),
        'status' => User::STATUS_INACTIVE,
        ]);

        Mail::to($user->email)->send(new VerifyMail($user));

        return $user;
}

public function register(Request $request)
{
        $this->validator($request->all())->validate();
        event(new Registered($user = $this->create($request->all())));

        return redirect()->route('login')
        ->with('success', 'Check your email and click on the link to verify.');
}

public function verify($token)
{
        if (!$user = User::where('verify_token', $token)->first()) {
        return redirect()->route('login')
        ->with('error', 'Sorry your link cannot be identified.');
        }

 $user->status = User::STATUS_ACTIVE;
        $user->verify_token = null;
        $user->save();

        return redirect()->route('login')
        ->with('success', 'Your e-mail is verified. You can now login.');
}
```

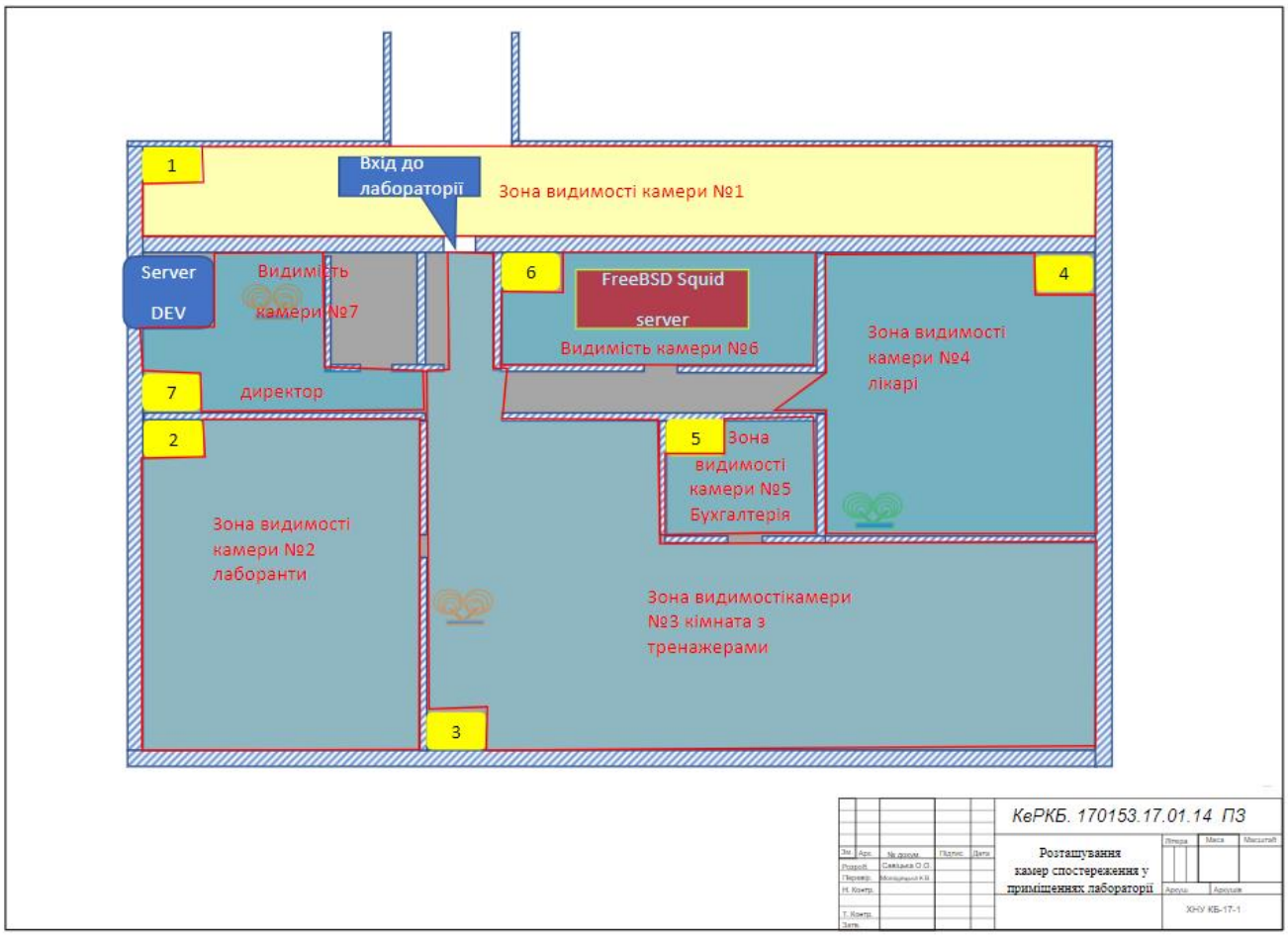
ДОДАТОК Б

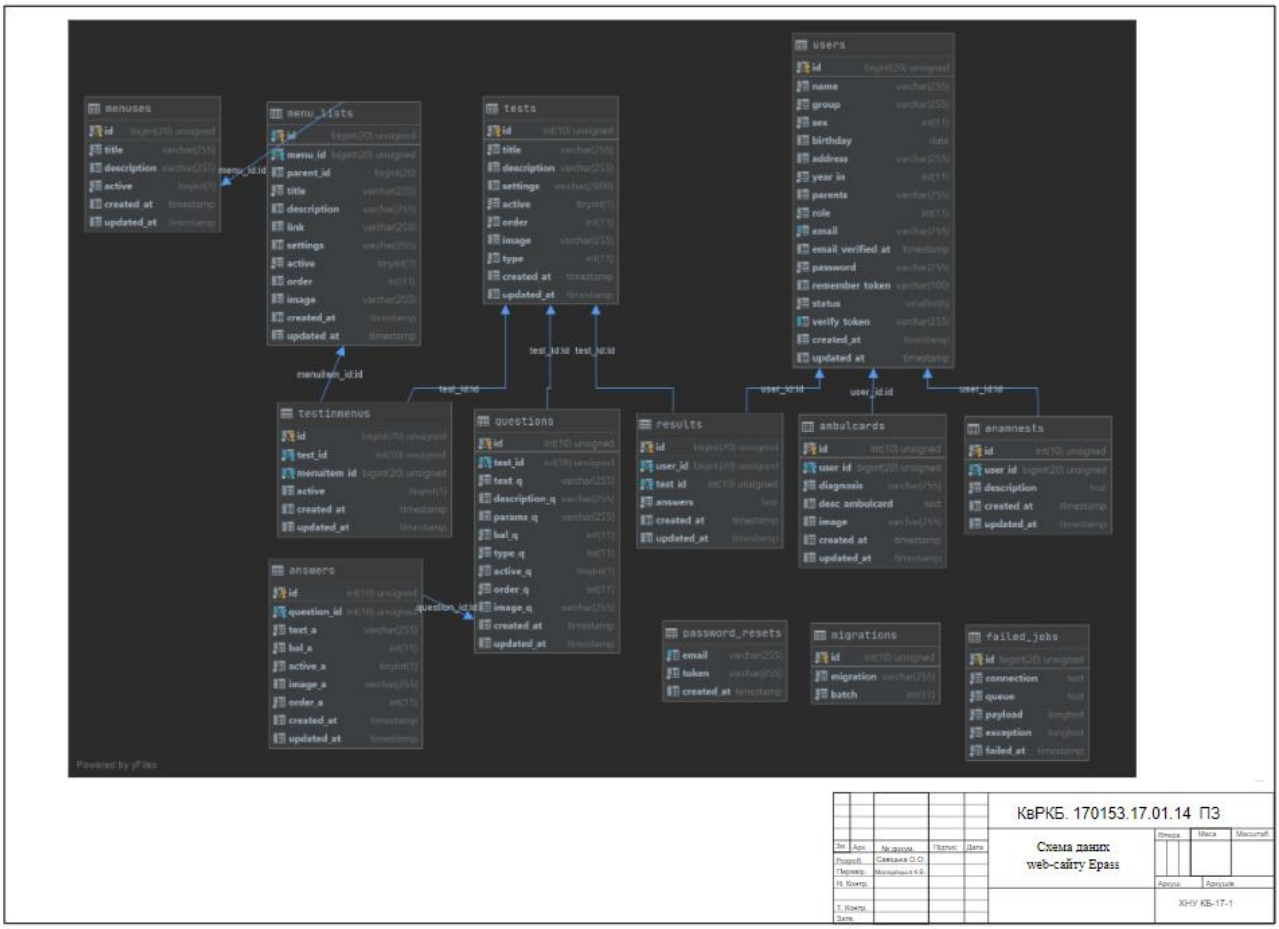
(Обов’язковий)

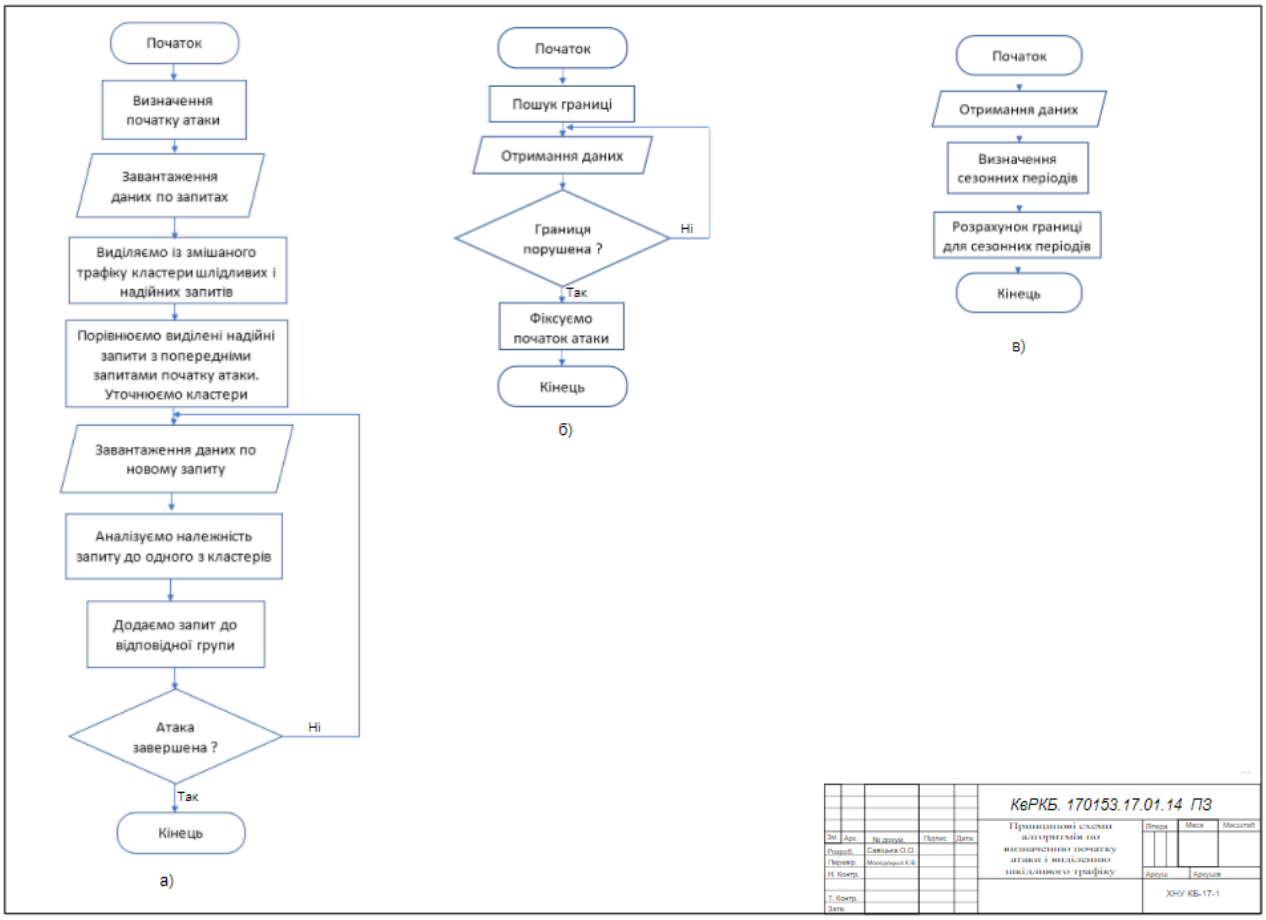
Копія графічної частини

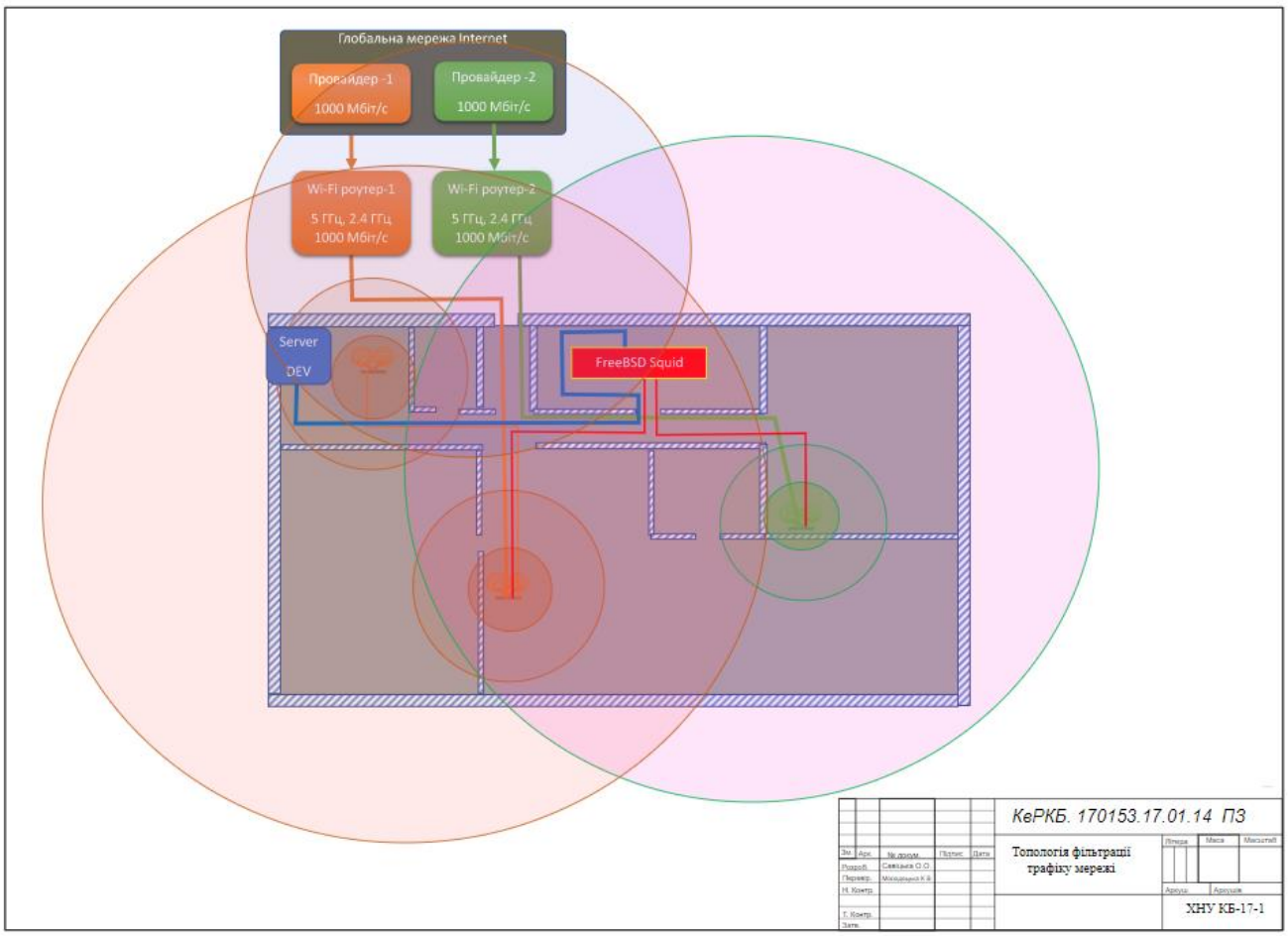





1
Вхід до лабораторії
Зона видимості камери №1
Server
DEV
Видимість
камери №7
6
FreeBSD Squid
server
Видимість камери №6
4
Зона видимості
камери №4
лікарі
7
директор
2
5
Зона
видимості
камери №5
Бухгалтерія
Зона видимості
камери №2
лаборанти
Зона видимостікамери
№3 кімната з
тренажерами
3
КвРКБ. 170153.17.01.14 ПЗ
Розташування
камер спостереження у
приміщеннях лабораторії
ХНУ КБ-17-1


menuses
menu_lists
tests
users
testinnenus
questions
results
ambulcards
anamnests
answers
password_resets
migrations
failed_jobs
КвРКБ. 170153.17.01.14 ПЗ
Схема даних
web-сайту Epass
ХНУ КБ-17-1


Початок
Визначення початку атаки
Завантаження даних по запитах
Виділяємо із змішаного трафіку кластери шкідливих і надійних запитів
Порівнюємо виділені надійні запити з попередніми запитами початку атаки. Уточнюємо кластери
Завантаження даних по новому запиту
Аналізуємо належність запиту до одного з кластерів
Додаємо запит до відповідної групи
Атака завершена ?
Ні
Так
Кінець
а)
Початок
Пошук границі
Отримання даних
Границя порушена ?
Ні
Так
Фіксуємо початок атаки
Кінець
б)
Початок
Отримання даних
Визначення сезонних періодів
Розрахунок границі для сезонних періодів
Кінець
в)
КвРКБ. 170153.17.01.14 ПЗ
Принципові схеми алгоритмів по виявленню початку атаки і виділенню шкідливого трафіку
ХНУ КБ-17-1


Глобальна мережа Internet
Провайдер -1
1000 Мбіт/с
Провайдер -2
1000 Мбіт/с
Wi-Fi роутер-1
5 ГГц, 2.4 ГГц
1000 Мбіт/с
Wi-Fi роутер-2
5 ГГц, 2.4 ГГц
1000 Мбіт/с
Server
DEV
FreeBSD Squid
КвРКБ. 170153.17.01.14 ПЗ
Топологія фільтрації трафіку мережі
ХНУ КБ-17-1

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ та контролю доступу до вебсайту «Електронний паспорт здоров'я студентів»

Автор: Савіцька Ольга Олегівна

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Керівник: Молодецька Катерина Валеріївна, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

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

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 1.9% що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ К.В. Молодецька

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

Дата: 07.06.2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студентка Савіцька Ольга Олегівна

Тема Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ та контролю доступу до Вебсайту «Електронний паспорт здоров'я студентів»

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 6; кількість сторінок записки 70

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі проведено аналіз виявлення вразливостей та загроз наявних на об'єкті захисту, з метою захисту на коректного функціонування наявного вебсайту, було модифіковано вебсайт на основі фреймворку Laravel та розроблено контроль доступу до нього.

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

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено огляд використовуваних в комп'ютерних системах методів захисту конфіденційної інформації, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі проведено аналіз системи захисту інформації навчально-наукової лабораторії медико-психологічних досліджень ХНУ, проаналізовано наявну систему захисту, виявлено канали витоку інформації. В третьому розділі проведено правовий та інженерно-технічний захист. У четвертому розділі було модифіковано наявний вебсайт на основі фреймворку Laravel та реалізовано контроль доступу до вебсайту.

4. Позитивні сторони роботи Слід відмітити позитивні сторони Кваліфікаційної роботи. Мета та цілі дослідження є актуальними і несуть комплексну практичну цінність. Актуальність обумовлена потребою у всебічному, комплексному захисті даних у різних галузях людської діяльності. Робота містить практичні аспекти виявлення вразливостей вебдодатків та їх усунення. Запропонований у роботі комплексний підхід до виявлення та захисту інформації можна розповсюдити на більшість вебсайтів, що дозволить уніфікувати системи захисту інформації.

5. Негативні сторони роботи З роботи не зрозуміло, чи піддається вебсайт атакам іншого роду окрім DDOS – атак, і яким чином в даній ситуації проводиться його захист. Не наведено вимоги до програмно апаратного забезпечення щодо ефективного функціонування вебсайта.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане якісно, з дотриманням чинних стандартів. Відповідно до теми кваліфікаційної роботи спостерігається загальна та професійна грамотність, лаконізм та логічна послідовність викладу матеріалу, органічний зв'язок текстового матеріалу з графічним. Текст пояснювальної записки розкриває ключові положення роботи, чіткий та лаконічний. Пояснювальна записка повністю відповідає вимогам до її змісту та оформлення і розкриває всі положення роботи.

7. Відгук про роботу в цілому В цілому кваліфікаційна робота заслуговує позитивної оцінки. Робота має прикладний характер. Матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи характеризуються логічною послідовністю викладення матеріалу, чіткістю та конкретністю результатів проектування, відповідають суті постановки завдання та меті кваліфікаційної роботи. Вдало підібрані методи дослідження, вірно прийняті рішення, розроблена система безпеки відповідає ТЗ і є повнофункціональною, використано сучасні засоби розробки та обґрунтовані висновки. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи.

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

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона виконана у повному обсязі із дотриманням вимог і заслуговує на оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) к.т.н, доцент, доцент каф. КІСП Мінєєв А.О.

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008205233

Check date:
07.06.2021 10:32:39 EEST

Check type:
Doc vs Internet

Report date:
07.06.2021 10:36:25 EEST

User ID:
100005590

File name: **Диплом_Савіцька**

Page count: **60** Word count: **10597** Character count: **81739** File size: **1.32 MB** File ID: **1008280928**

3.46% Matches

Highest match: **1.9%** with Internet source (http://elar.khnu.km.ua/jspui/bitstream/123456789/7660/1/11.pdf)

3.46% Internet sources	68	Page 62

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

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

Replaced characters	3

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 11%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 92419 Название: Аудит системи захисту навчально-наукової лабораторії медико-психологічних досліджень ХНУ та контролю доступу до Вебсайту «Електронний паспорт здоров'я студентів» Добавлено в БД: 2021-06-07 Авторы: Савіцька Ольга Руководители: Молодецька Катерина Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	72170	612	1496 (2%)	18 (3%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы