МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Кафедра програмування

ЛАБОРАТОРНА РОБОТА № 1

Дослідження методів захисту інформації на підприємстві.

Виконала:

Студентка групи ПМО-41

Кравець Ольга

Варіант: 15

Львів 2023

Варіант: 15.
Підприємство: проектний інститут.

Тема: Дослідження методів захисту інформації на підприємстві.

Мета: Отримати навички щодо аналізу організаційної структури та інформаційної інфраструктури підприємства, аналізу та вибору різних аспектів захисту інформації підприємства.

Хід роботи

Крок 1.

У цій лабораторній роботі я розглядаю підприємство “Львівський проектний інститут ”. Це приватне акціонерне товариство, розташоване у Франківському районі Львова та займається наданням послуг з інжинірингу, архітектурно-будівельного проєктування будівель і споруд I і II рівнів складності та проєктування лінійних об'єктів.

Одним із основних напрямків діяльності компанії ПрАТ ”Львівський проектний інститут” (ЛПІ) є надання послуг з архітектурно-будівельного проектування, а саме:

- об’єктів промислового призначення;
- громадських будівель та споруд;
- житлових будинків;
- інженерних споруд;
- проєктування інженерних систем (механічних, електротехнічних, сантехнічних, слабострумних);
- веж мобільного зв’язку.

ЛПІ також надають послуги у сферах інжинірингу, геології та геодезії:

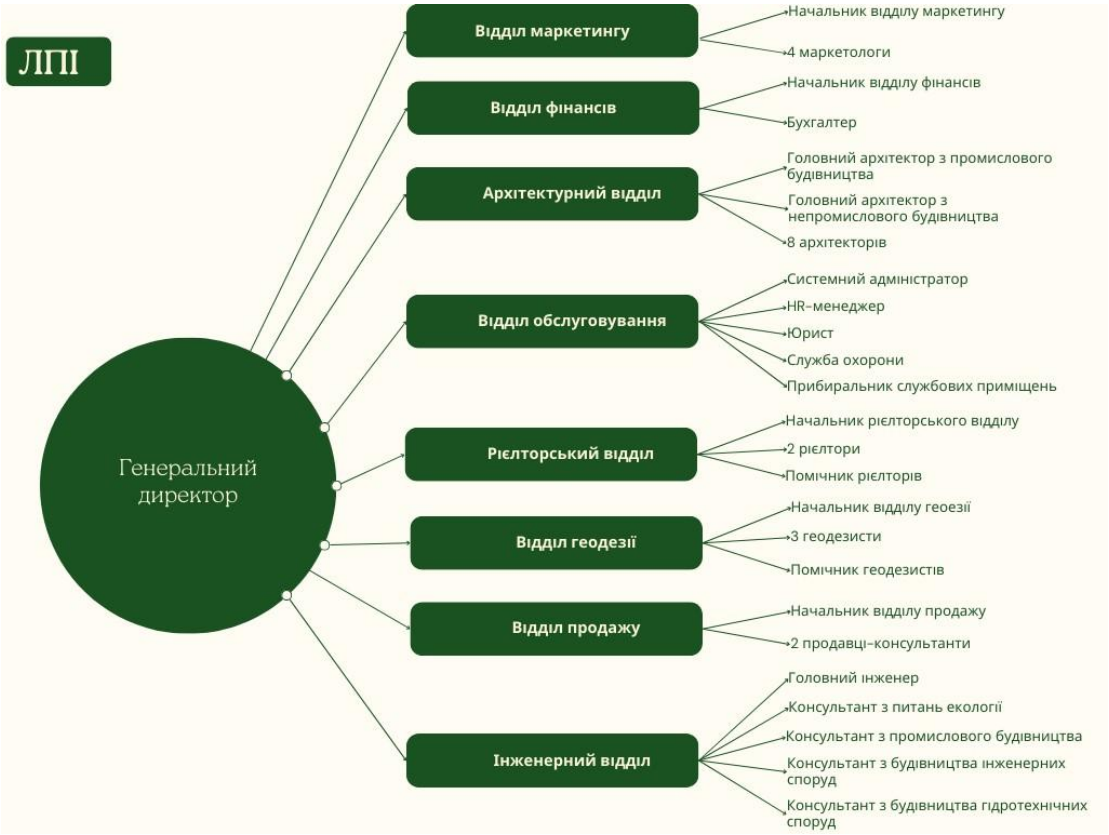
- інженерний дизайн та консультування: проектування промислового будівництва та гідротехнічниї споруд;
- діяльність у сфері інжинірингових послуг: нове будівництво, реконструкція об’єктів, технічне переоснащення, аудит витрат,

контроль якості робіт, обслуговування іноземних інвесторів, реалізації окремих функцій в будівництві;

- діяльність у сфері геодезії: вимірювання земельних ділянок та їх меж, роботи з вивчення підземних шарів, гідрологічні розвідувальні роботи;

- розроблення проєктів систем кондиціонування, охолодження, інженерні розробки щодо контролю санітарного стану та забруднення навколишнього середовища, боротьби із шумом і тд;

Середньооблікова кількість працюючих штатного складу - 42 людини.



Управлінська частина складається з:

1. Генеральний директор – людина, яка несе відповідальність за роботу підприємства в цілому.

2. Начальник відділ маркетингу - відповідальний за рекламу, роботу з клієнтами та пошук будівельних компаній.

3. Начальник відділу фінансів - відповідальний за роботу фінансового відділу, оформлення звітів та виплату заробітних плат.

4. Головний архітектор з промислового будівництва - відповідальний за роботу архітекторів з промислового будівництва.

5. Головний архітектор з непромислового будівництва - відповідальний за роботу архітекторів з непромислового будівництва.

6. Начальник рієлторського відділу - відповідальний за роботу рієлторського відділу.

7. Начальник відділу продажу - відповідальний за роботу інтернет-магазину.

8. Головний інженер - відповідальний за організацію роботи інженерного відділу.

9. Начальник відділу геодезії - відповідальний за організацію роботи

відділу геодезії.

Крок 2.

Розглянемо три рівні управління підприємством: стратегічний, тактичний та операційний.

1. Стратегічний рівень

На стратегічному рівні можна виділити 4 стратегії:

- технологічна стратегія (основна мета: ремонт та оновлення технологічного обладнання);
- фінансова стратегія (спрямована на збільшення доходів та ринкової вартості інституту);
- стратегія управління персоналом (спрямована на підвищення кваліфікації працівників);
- маркетингова стратегія (зосереджена на створенні якісної реклами підприємства та його послуг).

2. Тактичний рівень

Головною метою компанії є підвищення прибутку. Досягнення цієї цілі відбувається на тактичному рівні через створення плану, який включає послідовні інструкції, виконання яких призведе до збільшення статутного капіталу.

3. Операційний рівень

Керівники відділів повинні бути висококваліфікованими у відповідних галузях спеціалістами, здатними приймати рішення щодо стратегічного та тактичного рівня управління. Ці особи здатні швидко і якісно реагувати на можливі непередбачувані обставини, які можуть виникнути під час повсякденної роботи відділу. Також завданням керівника є забезпечення комфортного середовища праці в колективі для його підлеглих.

Крок 3.

Апаратне забезпечення підприємства:

- високоякісні потужні ноутбуки - 20 шт. (забезпечення роботи відділів геодезії, інженерного та архітектурного), Intel Core i7.
- Ноутбуки бізнес-класу - 20 шт.
- Монітори (4k Ultra HD) - 40 шт.
- Принтери - 10 шт.
- Факси - 4 шт.
- Жорсткі диски для збереження бекапу електронних даних.
- Amazon s3 Cloud Service для збереження даних компанії у хмарному середовищі.
- Допоміжна техніка: комп’ютерні миші, гарнітури, клавіатури, телефони.

Ноутбуки компанії обладнані Windows 11 Pro, пакетом Microsoft Office та програмами, що забезпечують роботу відповідного відділу.

Подача інтернет з’єднання відбувається за допомогою оптоволоконного кабелю з ціллю забезпечення стабільного та швидкісного з’єднання з мережею (200 Мбіт/с). Для забезпечення рівномірної подачі з’єднання до всіх частин офісу використовуються підсилювачі сигналу. Для доступу до зовнішніх серверів компанії, робоча техніка обладнана VPN (OpenVPN) з додатковим блокуванням сторонніх інтернет ресурсів.

Техніка є об’єднана у локальну мережу для швидкісної передачі даних у середині компанії. У кожного працівника є доступ до зовнішнього HardDrive відповідно до посадових обов’язків.

Крок 4.

Уся інформація підприємства поділяється на публічну та конфіденційну відповідно до діючого законодавства. До конфіденційної інформації належать: дані клієнтів, договори, проектні дані та особисті дані працівників компанії. До публічної інформації належить: політика підприємства, загальна інформація щодо компанії та її персоналу, фінансова звітність а також соціальні мережі підприємства, вебсайт тощо.

Документообіг компанії ведеться у електронному та паперовому форматі. Електронні копії документів зберігаються на HardDrive компанії та у хмарному середовищі. Паперові оригінали знаходяться на складі, відповідальність за який несе відділ фінансів та відділ обслуговування під контролем генерального директора.

Кожен комп’ютер обладнаний антивірусним програмним забезпеченням, ESET Endpoint Security. Вибір антивірусу базується на перевагах ESET Endpoint Security, зокрема кілька рівневим захистом ботнету, фаєрволом, додатковим захистом мобільної техніки та можливістю зовнішнього адмін контролю над мережею. Додаткове блокування сторонніх програм забезпечує безпеку даних робочої техніки.

У компанії існують такі засоби захисту:

- цілодобове відеоспостереження;
- бездротові пожежні датчики (Ajax Systems);
- бездротові охоронні пристрої (Ajax Systems);
- бездротові антипотоп-пристрої (Ajax Systems);
- джерела безперебійного живлення.

Крок 5.

Інформаційні ресурси	Доступність	Цілісність	Конфіденційність
Локальна мережа	**10/10.** *Доступ до локальної мережі компанії можливий лише з авторизованої робочої техніки для кожного працівника.*	**9/10.** *Структура даних та різнорівневий доступ до даних забезпечує цілісність інформації.*	**8/10.** *Безпека локальної мережі знаходиться у відповідальності системного адміністратора.*
Зовнішній HardDrive	**10/10.** *Доступ до даних можливий лише з авторизованої робочої техніки для кожного працівника відповідно до його посади.*	**10/10.** *Структура даних та різнорівневий доступ до даних забезпечує високу цілісність інформації.*	**8/10.** *Дані збережені на зовнішньому накопичувачі є відносно захищеними. Єдині способи втрати конфіденційності даних - у разі фізичної втрати накопичувача або порушення захищеності локальної мережі.*
Хмарне середовище	**8/10.** *Доступ до хмарного середовища можливий лише з робочої техніки.*	**10/10.** *Структура даних та різнорівневий доступ до даних забезпечує високу цілісність інформації.*	**9/10.** *Використання зовнішніх ресурсів Amazon забезпечує високий захист збережених даних.*
Робоча техніка	**10/10.** *Кожен працівник забезпечений*	**9/10.** *Допоміжна робоча техніка*	**9/10.** *Дані робочої техніки захищені*

	Робочою технікою відповідно до своїх посадових обов'язків.	*синхронізовано працює з основною, усі необхідні програмні ресурси встановлені та вчасно обновляються системним адміністратором*	*антивірусом.*
Вебсайт	**5/10.** *На даний момент компанія не є лідером ринку, відповідно вебсайт компанії не є результатом первинного пошуку для потенційних клієнтів.*	**5/10.** *Вебсайт компанії є по суті комбінацією інтернет-магазину та сайту-візитки.*	**8/10.** *Високий рівень захисту баз даних забезпечує високу конфіденційність даних вебсайту, хоча не можливо надати гарантію абсолютного захисту даних у випадку сторонніх атак на вебсайт.*

Крок 6.

Згідно до законодавства України робота підприємства підпорядковується:

- Відповідно до ст. 41 "Конституції" інформація є предметом державної охорони, яка забезпечується Законом України "Про інформацію", Законом України "Про захист інформації в автоматизованих системах" та ст. 361-363 Кримінального Кодексу України.
- "Положення про технічний захист в Україні" затверджено постановою Кабінету Міністрів України від 09.09.94 р. № 632.
- "Положення про порядок видачі суб'єктам підприємницької діяльності спеціальних дозволів (ліцензій) на здійснення окремих

видів діяльності” затверджено постановою Кабінету Міністрів України від 17.05.94 р. № 316.

- “Інструкція щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за її дотриманням” затверджена наказом ДСТСЗІ від 26.05.94 р. №46, зареєстровано в Мінюсті України 01.06.94 р. №120\329.
- “Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації” затверджено наказом ДСТСЗІ від 01.07.96 р. № 44, зареєстровано в Мінюсті України 18.07.96 р. № 366\1391.

Відповідно до “Помаранчевої книги” використовується клас інформаційної системи підприємства - С1, або клас вибіркового захисту, оскільки на підприємстві присутній поділ користувачів та даних. Тобто засоби управління здатні реалізувати обмеження до доступу, щоб захистити проект або приватну інформацію і не дати іншим користувачам випадково читати або руйнувати їх дані.

На підприємстві забезпечення ІБ відбувається завдяки наступним напрямкам:

- юридичний захист клієнтів та працівників компанії;
- безпека даних, що зберігає компанія (паперових та електронних).

Це досягається завдяки наступним механізмам:

- юридичний супровід роботи з клієнтами, наявність договорів про нерозголошення та згод на обробку персональних даних;
- наявність персоналу відповідального за безпеку даних;
- інструменти для забезпечення електронної безпеки даних;
- додаткові безпекові ресурси захисту фізичних даних компанії.

Організаційні засоби захисту, які використовуються:

1. Управління персоналом: розділення відповідальності та обов'язків, на яких базується доступ до даних кожного працівника з ціллю зменшити потенційний збиток від випадкових чи ненавмисних дій працівника.
2. Фізичний захист: збереження інформації у фізичному та електронному форматі, хмарному та фізичному; наявність засобів протипожежної безпеки та інших необхідних засобів забезпечення безпеки працівників.
3. Підтримка працездатності: система заохочень, преміювань та бонусів, створення корпоративної культури компанії.
4. Реагування на порушення режиму безпеки: наявність протоколу дій у якості виникнення витоку.

Вибір принципів керування компанії базується на різнопланових послугах, що надає підприємство. Умовно структура компанії поділяється на проектні відділи (відділ геодезії, інженерний відділ, тощо) та супутніми (фінансовий відділ, відділ маркетингу і тд.).

Проектні відділи забезпечують результативність виконання замовлень клієнтів, тоді як супутні надають підтримку у додаткових аспектах.

Заохочення та покарання працівників за порушення адміністративної безпеки повинні грунтуватись та базуватись на основі наступних чинників:

- ступінь критичності даних та кількість, що були поширені;
- мотивація працівника що спричинив порушення цілісності безпеки даних: умисне, ненавмисне, очікуване - для прикладу внаслідок проблем систем безпеки компанії;
- ознайомлення працівника з наслідками поширення інформації та те, що вона є конфіденційною;
- наявність юридичного регламентування безпеки даних.

В залежності від ступеня витоку адміністративними покараннями може бути звільнення працівника, притягнення до юридичної та адміністративної відповідальності, штраф, робоча догана.

Контроль території підприємства відбувається таким чином:

- забезпечення пропускної системи на територію;
- наявність служби охорони, що реагує у випадку небезпеки;
- наявність відеокамер спостереження та запису даних з них.

Пересування персоналу на території підприємства є вільним, з обмеженням фізичного доступу працівників до архіву, серверів (окрім працівників з відповідним рівнем доступу).

Щодо криптографічних та стеганографічних засобів, можна виділити:

- шифрування збережених даних задля безпеки баз даних компанії;
- контроль цілісності робочого програмного забезпечення та його вчасне оновлення;
- застосування електронного цифрового підпису для забезпечення юридичної значимості платіжних документів;

Спектр потенційних ризиків у разі порушення інформаційної безпеки підприємства є доволі широким. Зокрема, у випадку витоку особистих даних клієнта компанії, існує репутаційна загроза, а також ризик юридичного тиску на компанію, особливо якщо витік порушує умови договору з клієнтом. Також витік інформації про проєкти, що виконує компанія до конкурентів може спричинити відтік клієнтів та зниження конкурентоспроможності компанії у відповідній сфері діяльності.

Підсумовуючи, можна зробити висновок, загалом компанія “Львівський проектний інститут” має високий рівень інформаційної безпеки, який при тому не обмежує працездатність та результативність послуг, що надаються.

Компанія забезпечує інформаційну безпеку як клієнтів так і працівників на належному рівні. Ступінь захищеності не є максимальним, оскільки не виключає людський фактор та частково залежить від зовнішніх ресурсів. Проте, завдяки обмеженому доступу до інформації у працівників компанії та наявності стратегії контролю людського фактору, підприємство намагається мінімізувати ризики витоку з вищезгаданого боку.

Висновок:

На лабораторній роботі я отримала навички щодо аналізу організаційної структури та інформаційної інфраструктури підприємства, аналізу та вибору різних аспектів захисту інформації підприємства.