ЛАБОРАТОРНA РОБОТА № 1

**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.

Варіант-18. Типографія

Хід роботи

**Назва підприємства:** Типографія "Творча Літераль".

**Галузь діяльності:** Друкарня спеціалізується на друку різноманітної поліграфічної продукції, такої як книги, журнали, брошури, листівки, пакети, тощо.

**Розмір і місцезнаходження:** Підприємство розташоване в місті Київ і має велику площу для виробництва і складських потреб. У ньому працює близько 50 співробітників.

**Ринок і клієнти:** "Творча Літераль" обслуговує різні сектори ринку, включаючи видавничі компанії, рекламні агентства, корпорації, освітні установи та індивідуальних замовників.

**Продукція і послуги:** Підприємство надає послуги з друку на різних носіях, включаючи папір, картон, текстиль, а також різноманітні види обробки, такі як ламінація, спеціальне фарбування тощо.

**Управлінська структура:** Схема управління підприємством може бути поділена на кілька рівнів:

**Генеральний директор**: Вищий керівник підприємства, відповідальний за загальний стратегічний розвиток і прийняття ключових рішень.

**Відділ збуту і маркетингу:** Керує роботою з клієнтами, визначає цінову політику, веде маркетингові кампанії і розробляє стратегії розвитку ринків.

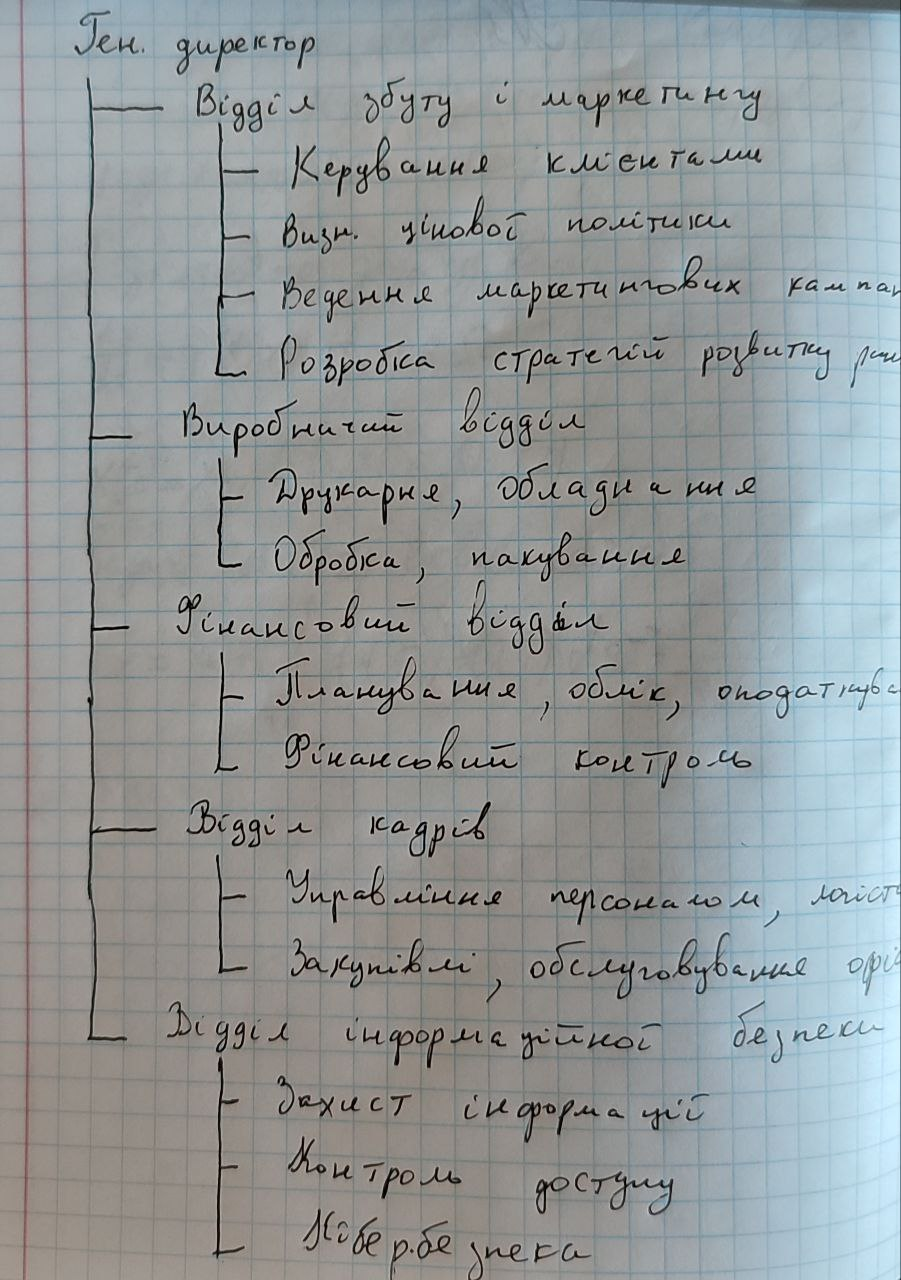
**Виробничий відділ:** Відповідає за виробництво поліграфічної продукції, включаючи друкарню, верстати, обробку і пакування.

**Фінансовий відділ:** Займається фінансовим плануванням, обліком, оподаткуванням та фінансовим контролем підприємства.

**Відділ кадрів і адміністративний відділ:** Відповідає за управління персоналом, а також адміністративні функції, включаючи логістику, закупівлі і обслуговування офісу.

**Відділ інформаційної безпеки:** Спеціалізується на забезпеченні захисту інформації підприємства, включаючи контроль доступу до даних, кібербезпеку та інші аспекти безпеки інформації.

Ця структура допомагає підприємству ефективно управляти всіма аспектами діяльності та забезпечувати якість продукції і безпеку інформації на підприємстві. Дослідження методів захисту інформації є важливим аспектом діяльності підприємства для забезпечення конфіденційності, цілісності та доступності важливої інформації.



2. Розглянемо аналіз структури та діяльності підприємства на різних рівнях управління: стратегічному, тактичному та операційному.

**Стратегічний рівень управління:**

На цьому рівні вирішуються загальні стратегічні питання, пов'язані з довгостроковим розвитком підприємства. Основні аспекти:

**Візія та місія підприємства:** Це визначається головною метою та цілями підприємства. Наприклад, візія може бути "стати лідером на ринку поліграфічних послуг", а місія - "надавати високоякісну поліграфічну продукцію з відмінним обслуговуванням".

**Стратегічне планування:** Розробка довгострокових стратегій розвитку, визначення конкурентних переваг, аналіз ринкових тенденцій та орієнтація на нові можливості.

**Політика безпеки та ризиків:** Вирішення питань щодо захисту інформації, ризиків та контролю над ними на стратегічному рівні.

**Тактичний рівень управління:**

На цьому рівні формулюються тактичні цілі та завдання для досягнення стратегічних цілей. Основні аспекти:

**Розробка бізнес-планів:** Створення конкретних планів та проектів, спрямованих на досягнення стратегічних цілей. Це може включати запуск нового продукту, розширення ринків або оптимізацію виробничих процесів.

**Фінансове управління:** Розробка бюджетів, управління фінансами, аналіз фінансової діяльності підприємства та прийняття відповідних фінансових рішень.

**Управління персоналом:** Вирішення питань з найму, навчання, розвитку та утримання персоналу, а також організація команди та розподіл обов'язків.

**Операційний рівень управління:**

Це рівень, на якому керівництво здійснює контроль та управління щоденною діяльністю підприємства. Основні аспекти:

**Виробничий процес і якість продукції:** Контроль якості та оптимізація виробничих процесів для досягнення високоякісної продукції.

**Запаси та логістика:** Ефективне управління запасами, логістичні операції та постачанням для забезпечення неперервності виробництва та вчасної поставки продукції.

Облік та звітність: Ведення фінансового та бухгалтерського обліку, складання звітів та забезпечення відповідності всіх фінансових операцій стандартам та законодавству.

Кожен з цих рівнів важливий для ефективного управління підприємством та досягнення стратегічних цілей. Взаємодія між цими рівнями дозволяє підприємству працювати гармонійно та ефективно на всіх рівнях управління.

3. Для аналізу стану інформатизації підприємства "Творча Літераль" розглянемо основні аспекти інформаційної технології на різних рівнях.

**Апаратне та програмне забезпечення:**

**Апаратне забезпечення:** Підприємство має сучасне обладнання для друку та обробки поліграфічної продукції. Включає в себе друкарні верстати, ламінатори, фальцеві машини та інше спеціалізоване обладнання. Серверне обладнання також присутнє для забезпечення роботи інформаційних систем.

**Програмне забезпечення:** Підприємство використовує спеціалізовані програми для друку та дизайну, такі як Adobe Creative Suite. Для обліку та фінансового управління використовується програмне забезпечення, наприклад, QuickBooks або внутрішні розробки.

**Локальна комп'ютерна мережа:**

Локальна комп'ютерна мережа підприємства "Творча Літераль" забезпечує зв'язок між працівниками та обладнанням. Основні характеристики мережі:

**Топологія:** Мережа побудована на основі зіркової топології, що сприяє надійності та простоті підтримки.

**Швидкість:** Мережа підтримує високу швидкість передачі даних, особливо між робочими станціями та серверами.

**Засоби захисту:** На рівні локальної мережі встановлені файерволи та системи інтегрованого контролю доступу для захисту внутрішньої мережі.

**Глобальний доступ:**

Підприємство "Творча Літераль" може мати доступ до глобальної мережі (Інтернету) для обміну даними та комунікацій. Основні аспекти:

**Інтернет-зв'язок:** Забезпечується стабільний та безпечний доступ до Інтернету, що дозволяє відправляти та отримувати електронну пошту, шукати інформацію, проводити онлайн-комунікації тощо.

**Захист від кібератак:** Встановлені системи виявлення та запобігання кібератак, антивірусне програмне забезпечення та регулярні аудити безпеки.

**Автоматизовані інформаційні системи:**

Підприємство використовує автоматизовані інформаційні системи для ефективного управління підприємством. Основні системи:

**Система управління замовленнями:** Допомагає у прийнятті, обробці та відстеженні замовлень від клієнтів, включаючи керування термінами виконання.

**Система обліку фінансів:** Для обліку фінансової діяльності, включаючи бюджетування, облік витрат і доходів.

**Система контролю якості:** Допомагає забезпечити якість друку та відслідковувати відхилення від стандартів.

Узагальнюючи, підприємство "Творча Літераль" має добре розвинуту інформаційну інфраструктуру, яка сприяє ефективній роботі та дозволяє виконувати основні функції друкарні. Важливою частиною цієї інфраструктури є заходи забезпечення безпеки інформації на різних рівнях.

4. На підприємстві "Творча Літераль" важливі інформаційні ресурси зосереджені як в паперовому, так і в електронному вигляді. Важливо забезпечити їхню надійну захист і зберігання. Ось деякі місця зосередження інформації та заходи захисту:

**Паперові інформаційні ресурси:**

**Офіси та робочі місця:** До паперових ресурсів відносяться документи, які обробляються на робочих столах працівників. Забезпечення безпеки включає в себе захист від несанкціонованого доступу, наприклад, через замки на шафках або обмеження фізичного доступу до приміщень.

**Архіви:** Паперові документи, які необхідно зберігати для обліку або законних вимог, зберігаються в спеціальних архівах. Для захисту важливо встановити систему критого зберігання, контролю доступу та реєстрацію видачі документів.

**Електронні інформаційні ресурси:**

**Сервери та дата-центр:** Електронні дані зазвичай зберігаються на серверах у дата-центрі підприємства. Заходи захисту включають в себе фізичну безпеку дата-центру, резервне копіювання, антивірусні програми та брандмауери.

**Робочі комп'ютери та ноутбуки:** Всі робочі станції та ноутбуки повинні бути захищені паролями та антивірусними програмами. Важливо також встановити політику безпеки паролів та шифрування даних на змінних носіях.

**Електронна пошта та комунікації:** Захист електронної пошти включає в себе фільтрацію спаму, антивірусні заходи та шифрування конфіденційних листів.

**Системи управління доступом:** Забезпечення контролю доступу до електронних ресурсів за допомогою паролів, двофакторної аутентифікації та управління правами доступу.

**Резервне копіювання:** Регулярне створення резервних копій важливих електронних даних і їх зберігання в безпечному місці.

**Шифрування даних:** Використання шифрування для захисту конфіденційних даних на серверах та в транзиті.

**Аудит інформаційної безпеки:** Проведення аудитів для виявлення можливих порушень безпеки та впровадження заходів для їх усунення.

Ці заходи спрямовані на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів підприємства.

5. З огляду на доступність, цілісність та конфіденційність інформаційних ресурсів підприємства "Творча Літераль", надаю таку оцінку:

**Доступність:** 8/10

Інформаційні ресурси в цілому є досить доступними. Підприємство має стабільний інтернет-зв'язок та локальну мережу, яка допомагає забезпечити швидкий обмін даними між працівниками. Однак є певні можливості для покращення доступності шляхом резервного забезпечення мережі і систем.

**Цілісність:** 9/10

Велика увага приділяється збереженню цілісності інформаційних ресурсів. Регулярне резервне копіювання та застосування антивірусного програмного забезпечення сприяють захисту від даних атак і втрати інформації. Проте, існують деякі можливості для покращення виявлення та відновлення даних в разі інциденту.

**Конфіденційність:** 7/10

Конфіденційність інформації в цілому забезпечена, але існують можливості для посилення захисту конфіденційних даних. Важливо підвищити свідомість працівників щодо безпеки даних та здійснювати більше заходів щодо контролю доступу до конфіденційної інформації.

Загалом, підприємство має добре організовану систему інформаційної безпеки, проте існують можливості для подальшого покращення, зокрема в аспектах контролю доступу та усунення можливих слабких місць в захисті інформації. Важливо продовжувати моніторити та апгрейдити інформаційну безпеку відповідно до зростаючих загроз.

6. Правовий захист інформації є критичним аспектом для забезпечення безпеки інформації на підприємстві. Наша країна має ряд законів та стандартів, якими підприємство повинно підпорядковуватись в галузі інформаційної безпеки (ІБ).

Ось деякі з них та рекомендації:

Закон України "Про захист інформації в інформаційних та телекомунікаційних системах": Цей закон встановлює загальні принципи і вимоги щодо захисту інформації в інформаційних та телекомунікаційних системах в Україні. Підприємство повинно дотримуватись цього закону, забезпечуючи відповідність своїх систем інформаційній безпеці.

Стандарт ISO 27001: Це міжнародний стандарт для управління інформаційною безпекою. Він встановлює рамки для розробки та впровадження системи управління інформаційною безпекою. Підприємство може використовувати цей стандарт для створення більш систематичного підходу до ІБ.

"Помаранчева книга" України: Ця книга визначає класифікацію інформації за рівнем конфіденційності і її зберігання. Підприємство повинно визначити клас своєї інформаційної системи відповідно до "Помаранчевої книги" і вживати відповідних заходів для захисту даних цього рівня.

Напрямки і механізми забезпечення ІБ на підприємстві можуть включати такі заходи:

**Політика і правила ІБ:** Розроблення і впровадження політики та правил ІБ, які встановлюють стандарти та процедури для захисту інформації на підприємстві.

**Шифрування даних:** Застосування шифрування для захисту конфіденційної інформації при зберіганні та передачі.

**Аудит безпеки:** Регулярний аудит системи ІБ для виявлення можливих слабких місць та потенційних загроз.

**Інформаційні заходи з навчання персоналу:** Навчання працівників правилам безпеки та свідомості щодо захисту інформації.

**Системи виявлення та запобігання вторгнень (IDS/IPS):** Встановлення систем для виявлення та запобігання несанкціонованим вторгненням у мережу підприємства.

**Засоби антивірусної захисту:** Використання антивірусного програмного забезпечення для виявлення та блокування загроз.

Регулярне оновлення програмного забезпечення та патчів: Постійне оновлення і патчизація програмного забезпечення для запобігання використанню вразливостей.

**Захист фізичних ресурсів:** Забезпечення фізичної безпеки серверних приміщень та обладнання.

Застосовуючи ці напрямки і механізми, підприємство може створити більш комплексну систему інформаційної безпеки, яка відповідає його потребам і вимогам законодавства України.

Організаційний захист інформації:

Організаційний захист інформації на підприємстві "Творча Літераль" включає в себе ряд заходів та структури, спрямованих на забезпечення безпеки інформації.

Основні заходи організаційного рівня:

**Розробка політики безпеки:** Створення документа з описом правил та вимог щодо захисту інформації на підприємстві.

**Управління доступом:** Встановлення процедур для надання та зняття доступу до інформаційних ресурсів на підприємстві.

**Засоби аудиту безпеки:** Впровадження системи аудиту, яка дозволяє відстежувати та аналізувати дії користувачів і систему для виявлення можливих загроз.

**Навчання та свідомість персоналу:** Проведення навчання з питань безпеки інформації для всього персоналу, а також створення свідомої культури безпеки.

**Моніторинг інцидентів і реагування:** Створення процедур для виявлення, реєстрації та вирішення інцидентів, пов'язаних із загрозами інформаційної безпеки.

Принципи керування персоналом:

**Принцип необхідності доступу:** Кожен працівник отримує доступ лише до тих інформаційних ресурсів, які необхідні для виконання його робочих обов'язків.

**Принцип надійності паролів:** Вимагати від працівників використовувати складні паролі та регулярно їх змінювати.

**Принцип обмеженого доступу:** Забороняти працівникам доводити конфіденційну інформацію до третіх осіб без належного дозволу.

Правила заохочення та покарання:

**Заохочення:** Встановити систему винагород та визнання за відмінність в питаннях інформаційної безпеки, наприклад, бонуси чи похвальні листи.

**Покарання:** Визначити санкції за порушення правил інформаційної безпеки, такі як дисциплінарні заходи чи втрата привілеїв доступу.

**Засоби фізичного захисту і керування доступом:**

Системи контролю доступу: Встановлення системи кард-код доступу до приміщень і обладнання.

**Замки і об'єкти які розглядаємо:** Забезпечення фізичного захисту серверних приміщень та архівів.

Структура служби безпеки:

Служба безпеки на підприємстві може складатися з таких підрозділів:

**Аналіз ризиків і безпеки:** Відповідає за оцінку ризиків і розробку стратегій інформаційної безпеки.

**Технічна підтримка інфраструктури безпеки:** Забезпечує функціонування та підтримку технічних засобів безпеки.

**Навчання і свідомість:** Організовує навчання та інформує персонал про важливість інформаційної безпеки.

**Відповідь на інциденти:** Визначає процедури реагування на інциденти та їх подальше розслідування.

Інженерно-технічний захист інформації включає в себе різні заходи та технології для забезпечення безпеки підприємства від зовнішніх загроз та недозволених дій персоналу. Ось деякі інженерно-технічні рішення, які відповідають політиці безпеки:

Контроль території підприємства:

Відеоспостереження: Встановлення камер важливих точок на території підприємства для нагляду та реєстрації подій. Дані з камер можуть бути записані та архівовані для подальшого аналізу.

Датчики руху і периметральні системи безпеки: Використання датчиків руху та систем сповіщення про вторгнення, які можуть спрацьовувати при незаконному проникненні на територію підприємства.

Контроль за пересуванням персоналу:

Магнітні картки або смарт-карти для автентифікації: Використання таких карток для забезпечення доступу працівників лише до відповідних приміщень або ресурсів.

Біометричні системи: Встановлення системи біометричної ідентифікації (відбитки пальців, розпізнавання обличчя) для підвищення безпеки при доступі до об'єктів.

Технічні засоби захисту:

Пожежна сигналізація та системи протипожежного захисту: Встановлення системи, яка спрацьовує при виникненні пожежі та вчасно інформує про це працівників та служби безпеки.

Системи контролю доступу: Використання систем, які контролюють фізичний доступ до приміщень та об'єктів.

Захищені мережі Wi-Fi: Забезпечення безпеки мережі Wi-Fi шляхом шифрування трафіку та використання аутентифікації.

Криптографічні та стеганографічні засоби:

Шифрування даних: Використання криптографічних алгоритмів для захисту конфіденційної інформації під час передачі та зберігання.

Стеганографія: Вбудовання інформації в інші медіафайли для прихованої передачі.

Програмно-технічний захист інформації включає в себе використання програмних рішень та технологій для захисту інформації на підприємстві. З огляду на розроблену політику безпеки, ось деякі програмні рішення та їх оцінка ризиків:

Антивірусний контроль:

**Програмне рішення:** Встановлення робочого антивірусного програмного забезпечення на всіх робочих станціях та серверах.

**Ризики:** Без антивірусного захисту, підприємство вразливе перед вірусами, шкідливими програмами та загрозами з Інтернету.

Шифрування:

**Програмне рішення:** Використання програм для шифрування файлів та даних, що зберігаються на серверах і пристроях.

**Ризики:** Без шифрування інформація може бути підвернута ризику під час передачі та зберігання.

Автентифікація на робочому місці:

**Програмне рішення**: Встановлення системи автентифікації для кожного користувача на робочих станціях.

**Ризики:** Без системи автентифікації можуть виникнути проблеми з несанкціонованим доступом до інформації.

Оцінка ризиків:

З урахуванням вищезазначених програмних рішень, ризики можуть бути зменшені до мінімуму:

**Ризики без антивірусного контролю:** Велика ймовірність втрати даних або поширення вірусів і шкідливих програм. Розповсюдження вірусів може призвести до відмови систем та витрат на відновлення.

**Ризики без шифрування:** Конфіденційна інформація може бути доступною для несанкціонованих осіб при перехопленні або витоку даних.

**Ризики без системи автентифікації:** Можливість несанкціонованого доступу до робочих станцій та даних, що зберігаються на них.

Висновки щодо ефективності захисту:

Запропоновані програмні рішення, такі як антивірусний контроль, шифрування та системи автентифікації, є ефективними засобами для зменшення ризиків інформаційної безпеки на підприємстві. Вони допоможуть у запобіганні втрати даних, незаконному доступу та іншим загрозам. Проте важливо не забувати про постійне оновлення та моніторинг цих рішень для забезпечення їхньої актуальності та ефективності перед новими загрозами.