Міністерство освіти і науки України
Національний Університет «Львівська політехніка»
Кафедра СВР

Лабораторна робота №1
з дисципліни: «Інформаційна безпека даних у видавничій галузі»
на тему:
«Аналіз структури та діяльності підприємства на різних рівнях деталізації»

Виконав:
ст. гр. Кн-22д
Теслюк Тимофій
Перевірила:
д. т. н., доц. Кудряшова А. В.

Львів-2025

Завдання 1

ASUS – тайванська міжнародна компанія, заснована в 1989 році, яка

спеціалізується на виробництві комп'ютерного обладнання та споживчої електроніки.

- Компанія пропонує широкий спектр продукції, включаючи:
- персональні комп'ютери;
- ноутбуки;
- монітори;
- проєктори;
- материнські плати;
- відеокарти;
- оптичні накопичувачі;
- периферійні пристрої;
- носимі пристрої;
- сервери;
- смартфони;
- мережеве обладнання.

Завдання 2

ASUS має **ієрархічно-функціональну структуру управління** з елементами дивізійного підходу. Це означає, що компанія поділяється на окремі функціональні підрозділи (наприклад, виробництво, маркетинг, фінанси, продажі), які підпорядковуються центральному керівництву.

Ключові рівні управління:

- **Генеральний директор (CEO)** – відповідає за загальну стратегію, розвиток компанії та ухвалення ключових рішень.
- **Виконавчий директор (COO)** – контролює операційну діяльність, координацію між підрозділами.
- **Фінансовий директор (CFO)** – управляє фінансами, інвестиціями, ризиками та бюджетуванням.
- **Функціональні директори (CMO, CSO тощо)** – керують відповідними напрямами (маркетинг, продажі, виробництво).

Завдання 3

У компанії **ASUS** важливі інформаційні ресурси – як **паперові**, так і **електронні** – зберігаються централізовано та з урахуванням найвищих стандартів інформаційної безпеки. Ось як це виглядає:

Паперові інформаційні ресурси:

- **в головному офісі ASUS у Тайбеї (Тайвань)** – тут розташовані архіви корпоративної документації, стратегічних планів, фінансових звітів та інших важливих паперових документів;
- **в юридичних та фінансових відділах** – документація щодо контрактів, договорів, звітності;
- **на виробничих підприємствах і логістичних центрах** – технічні специфікації, супровідна документація, сертифікати якості тощо.

Паперові архіви ASUS організовані з урахуванням політик доступу та тривалого зберігання, згідно з міжнародними стандартами.

Електронні інформаційні ресурси:

- **у корпоративних дата-центрах** (основний у Тайвані, резервні – у Європі, США та Азії);
- **у хмарних сервісах** (ASUS активно використовує хмарну інфраструктуру для зберігання даних, резервного копіювання, роботи з клієнтами);

- **на внутрішніх серверах підрозділів** – наприклад, сервери відділу R&D зберігають розробки, тестові дані, технічну документацію;
- **у системах ERP (Enterprise Resource Planning)** – там зберігаються всі основні бізнес-дані: фінанси, логістика, запаси, управління персоналом тощо.

ASUS активно використовує **власні засоби захисту**, зокрема антивірусні рішення та системи контролю доступу, а також співпрацює з провідними IT-компаніями для підвищення кібербезпеки.

Завдання 4

1. **Доступність:**

- Найвищий рівень доступності у **хмарних сервісів** (10/10), оскільки до них можна отримати доступ звідусіль.
- **Дата-центри** та **ERP-система** (9/10) забезпечують високу швидкість роботи.
- **Паперові архіви** (6/10) мають найнижчий показник, оскільки потребують фізичного доступу.

2. **Цілісність:**

- **ERP-система** має найвищий рівень цілісності (10/10) завдяки резервному копіюванню та жорсткому контролю змін.
- **Паперові архіви** (8/10) ризикують через фізичний знос документів.
- **Хмарні сервіси** (8/10) можуть бути вразливими до збоїв у мережі.

3. **Конфіденційність:**

- **Дата-центри, ERP-система та внутрішні сервери** мають високий рівень захисту (9/10) завдяки багаторівневій автентифікації та шифруванню.
- **Паперові архіви** (7/10) можуть бути викрадені або пошкоджені, що знижує рівень конфіденційності.

Таким чином ASUS має добре організовану систему зберігання та захисту інформації. Найкращі показники мають ERP-системи та дата-центри, які забезпечують високу доступність, цілісність і конфіденційність. Найвразливішими залишаються паперові архіви, що мають низьку доступність і підвищені ризики втрати інформації.

Завдання 5

1. Важливість інформації як активу

Компанія ASUS є світовим лідером у сфері комп'ютерних технологій. Вона володіє величезними масивами даних, зокрема:

- комерційною та фінансовою інформацією (контракти, звіти, інвестиції);
- інтелектуальною власністю (патенти, розробки, технології);
- персональними даними клієнтів і співробітників;
- логістичною інформацією (ланцюги поставок, постачальники, партнери).

Втрата або компрометація цих даних може завдати значних збитків компанії.

2. Основні загрози інформаційній безпеці

ASUS, як і будь-яка велика технологічна корпорація, піддається наступним ризикам:

- Кіберзлочинність – хакерські атаки, DDoS, віруси та зловмисне ПЗ.
- Індустріальне шпигунство – конкурентна розвідка, витоки даних.
- Внутрішні загрози – недбалість або зловмисні дії співробітників.
- Фізичні загрози – зломи офісів, крадіжка носіїв інформації.
- Форс-мажори – пожежі, природні катаклізми, технічні збої.

3. Доцільність комплексної системи захисту інформації

- Підвищення рівня довіри з боку клієнтів, партнерів та інвесторів.
- Захист інтелектуальної власності, що є ключовим активом компанії.
- Дотримання міжнародних стандартів (ISO/IEC 27001, GDPR, CCPA).
- Запобігання фінансовим втратам унаслідок атак та витоків даних.
- Забезпечення стабільності роботи компанії без зовнішніх і внутрішніх загроз.

4. Основні заходи щодо покращення безпеки

- Шифрування даних – застосування передових методів для захисту файлів і комунікацій.
- Посилена аутентифікація – використання двофакторної та біометричної перевірки доступу.

– Захист хмарних сховищ – налаштування безпечних VPN, обмеження доступу до критичних даних.

– Моніторинг і аудит – аналіз логів доступу, виявлення аномальної активності.

– Навчання персоналу – програми підвищення обізнаності про кібербезпеку.

– Фізичний захист серверів – обмежений доступ до дата-центрів, системи відеоспостереження.

Розробка комплексної системи захисту інформації є необхідною та доцільною, оскільки це гарантує стабільність, конкурентоспроможність та довіру до компанії ASUS. Інвестування в кібербезпеку та захист інформації допоможе мінімізувати ризики та забезпечити довгостроковий успіх компанії на глобальному ринку.

Завдання 6

Висновки щодо аналізу інформаційних ресурсів та захисту інформації в ASUS

1. Структура управління та інформаційні ресурси ASUS

Аналіз організаційної структури компанії ASUS показав, що вона має ієрархічно-функціональний підхід до управління, що забезпечує чіткий розподіл відповідальності. Інформаційні ресурси компанії представлені в паперовому та електронному вигляді, причому цифрові дані домінують, що відповідає сучасним бізнес-реаліям. Компанія орієнтована на високотехнологічні рішення, зберігаючи при цьому традиційні механізми документообігу.

2. Оцінка інформаційних ресурсів за критеріями доступності, цілісності та конфіденційності

Оцінювання показало, що найбільш захищеними є корпоративні дата-центри, які мають високі показники доступності (9/10), цілісності (9/10) та конфіденційності (9/10). Хмарні технології отримали трохи нижчі оцінки через залежність від зовнішніх провайдерів. Паперові архіви мають обмежену доступність і потребують додаткового фізичного захисту. Електронні ресурси

ASUS захищені набагато краще, ніж паперові, що вказує на необхідність оптимізації фізичного документообігу.

3. Необхідність посилення інформаційної безпеки

Аналіз загроз показав, що ASUS, як глобальна технологічна корпорація, піддається кіберзлочинності, індустріальному шпигунству та внутрішнім ризикам. Сучасні виклики вимагають розширення заходів захисту. Підприємству необхідно постійно вдосконалювати систему безпеки, інтегруючи захищені хмарні рішення, посилений моніторинг трафіку та навчання персоналу.

Загальний висновок:

– ASUS ефективно використовує сучасні інформаційні технології, але потребує подальшої оптимізації управління паперовими архівами.

– Оцінка ресурсів показала високий рівень захисту електронних даних, що відповідає міжнародним стандартам.

– Подальший розвиток системи безпеки має бути стратегічним пріоритетом, щоб забезпечити захист даних, конкурентоспроможність та довіру до бренду.

– Розробка комплексної системи захисту інформації є не просто необхідністю, а критично важливим фактором стабільності та довгострокового успіху компанії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційний сайт компанії ASUS Україна. https://www.asus.com/ua-ua/

2. Політика конфіденційності ASUS. https://www.asus.com/ua-ua/terms_of_use_notice_privacy_policy/privacy_policy

3. Матеріал з Вікіпедії https://uk.wikipedia.org/wiki/ASUS