## Тема 4. Безпека та управління даними в цифровому обліку

1.1 Захист даних в умовах цифрової трансформації: виклики та перспективи.

1.2 Управління доступом до даних та їх інтегрованість.

1.3 Стандарти та регулювання в галузі цифрової трансформації обліку.

***Основні терміни та поняття:*** *захист даних, цифрова трансформація, кібербезпека, персональні дані, кібератаки, штучний інтелект, блокчейн, управління доступом до даних, інтегрованість даних, кібербезпека, інформаційна безпека, стандарти, регулювання, МСФЗ, GDPR, COSO.*

### 4.1 Захист даних в умовах цифрової трансформації: виклики та перспективи.

Цифрова трансформація, що охопила всі сфери життя, суттєво змінила підходи до збору, обробки та зберігання даних. З одного боку, це відкрило нові можливості для розвитку бізнесу, науки та суспільства в цілому. З іншого боку, створило безпрецедентні виклики для захисту даних, особливо персональних.

Актуальність проблеми

Захист даних став одним з найгостріших питань сучасності. Збільшення кількості кібератак, викрадення персональних даних, фінансові втрати компаній та держав – все це підкреслює необхідність надійного захисту інформації.

Основні виклики:

- Збільшення обсягів даних: Експоненціальне зростання обсягів даних, що збираються, обробляються та зберігаються, ускладнює їх захист.
- Різноманітність загроз: Кібератаки стають все більш складними та витонченими, з’являються нові типи загроз.
- Розвиток технологій: Нові технології, такі як штучний інтелект та машинне навчання, з одного боку, відкривають нові можливості для захисту даних, але з іншого – можуть бути використані злочинцями.
- Міжнародна природа загроз: Кібератаки можуть здійснюватися з будь-якої точки світу, що ускладнює їх відстеження та припинення.
- Законодавчі прогалини: Існуюче законодавство часто не встигає за розвитком технологій і не завжди забезпечує адекватний захист даних.

Заходи щодо захисту даних:

- Технічні засоби захисту: Системи виявлення вторгнень, антивірусні програми, шифрування даних, двофакторна аутентифікація тощо.
- Організаційні заходи: Розробка політики безпеки, навчання персоналу, регулярне тестування систем безпеки.
- Законодавче регулювання: Прийняття та вдосконалення законодавства, що регулює захист персональних даних.
- Міжнародне співробітництво: Створення міжнародних механізмів співпраці в галузі кібербезпеки.

Перспективи розвитку:

• Розвиток технологій захисту даних: Штучний інтелект може бути використаний для прогнозування кібератак та автоматизації процесів захисту.

• Блокчейн: Технологія блокчейн може забезпечити високий рівень безпеки та прозорості при зберіганні даних.

• Квантова криптографія: Розвиток квантових комп'ютерів може призвести до створення незламних систем шифрування.

• Збільшення відповідальності компаній: Компанії будуть нести більшу відповідальність за захист персональних даних своїх клієнтів.

Захист даних є одним з найважливіших викликів сучасності. Для забезпечення ефективного захисту даних необхідно поєднувати зусилля держави, бізнесу та громадянського суспільства. Тільки спільними зусиллями ми зможемо створити безпечне цифрове середовище.

*Детальний опис тем*

Вплив штучного інтелекту на кібербезпеку

Штучний інтелект (ШІ) революціонізує багато галузей, і кібербезпека не є винятком. ШІ може бути використаний як для захисту, так і для атак.

Позитивні аспекти:

• Виявлення загроз: ШІ-системи можуть аналізувати великі обсяги даних у реальному часі, виявляючи аномалії та потенційні загрози, які можуть бути пропущені людським оком.

• Проактивна оборона: ШІ може прогнозувати майбутні атаки на основі історичних даних, дозволяючи приймати превентивні заходи.

• Автоматизація рутинних завдань: ШІ може автоматизувати багато рутинних завдань, таких як сканування на наявність шкідливого програмного забезпечення, що дозволяє фахівцям з кібербезпеки зосередитися на більш складних завданнях.

Негативні аспекти:

• Створення нових загроз: Зловмисники можуть використовувати ШІ для створення більш складних і витончених атак, таких як генерація глибоких підробок або розробка самонавчальних шкідливих програм.

• Ризик упередженості: ШІ-системи навчаються на даних, які можуть містити упередження, що може призвести до помилкових спрацювань або пропусків реальних загроз.

Роль блокчейну в захисті персональних даних

Блокчейн – це розподілена база даних, яка зберігає інформацію в блоках, що з'єднані між собою криптографічними хешами. Ця технологія має ряд переваг для захисту персональних даних:

• Незмінність даних: Інформація, записана в блокчейн, є практично незмінною, що ускладнює її підробку або видалення.

• Прозорість: Усі транзакції в блокчейні є публічними, що забезпечує високий рівень прозорості.

• Децентралізація: Блокчейн не контролюється жодним централізованим органом, що робить його більш стійким до атак.

Застосування блокчейну:

- Ідентифікація: Блокчейн може використовуватися для створення децентралізованих систем ідентифікації, що дозволяють користувачам контролювати свої персональні дані.
- Зберігання медичних даних: Блокчейн може забезпечити безпечне та конфіденційне зберігання медичних даних пацієнтів.
- Захист авторських прав: Блокчейн може використовуватися для реєстрації та захисту авторських прав на цифрові активи.

Правові аспекти захисту даних в умовах цифрової трансформації

Цифрова трансформація поставила перед законодавцями нові виклики, пов'язані із захистом персональних даних. Основні аспекти правового регулювання:

- Загальний регламент про захист даних (GDPR): Європейський союз прийняв GDPR, який встановлює високі стандарти захисту персональних даних.
- Національне законодавство: Більшість країн мають свої закони про захист персональних даних, які можуть доповнювати або уточнювати GDPR.
- Принципи захисту даних: Законність, добросовісність, прозорість, обмеження цілей, мінімізація даних, точність, обмеження зберігання, цілісність та конфіденційність.
- Права суб'єктів персональних даних: Право на доступ, виправлення, видалення, обмеження обробки, переносимість даних, заперечення, автоматизоване прийняття рішень та профілювання.
- Відповідальність: За порушення законодавства про захист персональних даних передбачена адміністративна, цивільна та кримінальна відповідальність.

Кібербезпека критичної інфраструктури

Критична інфраструктура – це системи та активи, від безперебійної роботи яких залежить життєдіяльність суспільства. Кібератаки на критичну інфраструктуру можуть мати серйозні наслідки, такі як збої в енергопостачанні, транспорті, комунікаціях тощо.

Основні загрози:

- Вимога викупу: Зловмисники шифрують дані критично важливих систем і вимагають викуп за їх розшифрування.
- Саботаж: Зловмисники можуть намагатися вивести з ладу критичну інфраструктуру з метою дестабілізації суспільства.
- Шпіонаж: Зловмисники можуть використовувати кібератаки для отримання доступу до конфіденційної інформації.

Заходи захисту:

- Посилення фізичної безпеки: Захист об'єктів критичної інфраструктури від несанкціонованого доступу.
- Регулярне оновлення програмного забезпечення: Усунення вразливостей, які можуть бути використані зловмисниками.
- Створення резервних копій: Регулярне створення резервних копій даних для відновлення у разі втрати.
- Співпраця з правоохоронними органами: Обмін інформацією про кіберзагрози та координація дій у разі інцидентів.

Захист даних в умовах цифрової трансформації є складним і багатогранним завданням. Для його вирішення необхідні спільні зусилля держави, бізнесу та громадянського суспільства. Тільки за умови ефективного захисту даних ми зможемо повною мірою реалізувати потенціал цифрових технологій.

Таблиця 4.1 - Порівняльний аналіз законодавства різних країн щодо захисту персональних даних

| Країна | Основний закон про захист персональних даних | Ключові принципи | Особливості |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Європейський Союз | Загальний регламент про захист даних (GDPR) | Законність, добросовісність, прозорість, обмеження цілей, мінімізація даних, точність, обмеження зберігання, цілісність та конфіденційність, відповідальність | Високі стандарти захисту, екстериторіальна дія, значні штрафи за порушення |
| США | Закони штатів, федеральні закони (HIPAA, CCPA, GDPR для компаній, що працюють на європейському ринку) | Різноманітність законодавства, фокус на конкретних секторах (медицина, фінанси) | Менш єдиний підхід, ніж в ЄС, але тенденція до посилення захисту даних |
| Канада | Закон про захист персональних даних і електронні документи (PIPEDA) | Принципи, схожі на GDPR, але з деякими відмінностями | Широкий спектр застосування, включаючи федеральні установи та приватні компанії |
| Австралія | Закон про приватність 1988 року | Принципи, схожі на GDPR, але з деякими відмінностями | Сильний акцент на прозорості та звітності |
| Японія | Закон про захист персональних інформаційних активів | Принципи, схожі на GDPR, але з деякими відмінностями | Фокус на захисті інформації, що стосується громадян Японії |

| | | | |
|---|---|---|---|
| Китай | Закон про захист персональних даних (запроваджений у 2021 році) | Принципи, схожі на GDPR, але з акцентом на національну безпеку | Строгий контроль держави за обробкою персональних даних |
| Україна | Закон України "Про захист персональних даних" | Законність обробки, добросовісність, прозорість, точність, обмеження цілей, зберігання, цілісність та конфіденційність | Постійне вдосконалення законодавства, вплив європейських стандартів |

Особливості законодавства України про захист персональних даних

- Закон України "Про захист персональних даних": Основний нормативно-правовий акт, що регулює відносини у сфері захисту персональних даних.
- Вплив європейського законодавства: Українське законодавство формувалось під впливом європейських стандартів, зокрема GDPR, що сприяло підвищенню рівня захисту персональних даних.
- Постійне вдосконалення: Закон регулярно доповнюється та змінюється з метою адаптації до нових викликів і технологічних рішень.
- Роль Уповноваженого Верховної Ради України з прав людини: Цей орган здійснює контроль за дотриманням законодавства про захист персональних даних.
- Виклики: Недостатня обізнаність громадян та суб'єктів господарювання про свої права та обов'язки у сфері захисту персональних даних, а також необхідність подальшого вдосконалення механізмів контролю та відповідальності.

Ключові відмінності українського законодавства від GDPR:

- Менш деталізовані вимоги: Деякі положення українського закону є менш деталізованими, ніж у GDPR.
- Інші підходи до деяких питань: Є відмінності в підходах до таких питань, як згода суб'єкта персональних даних, обґрунтування законних інтересів та ін.
- Менші штрафи за порушення: Штрафи за порушення законодавства про захист персональних даних в Україні, як правило, нижчі, ніж у ЄС.

Загальна тенденція: Українське законодавство про захист персональних даних розвивається в напрямку гармонізації з європейськими стандартами. Це сприяє підвищенню рівня захисту персональних даних громадян України та посиленню довіри до українських компаній серед міжнародних партнерів.

### 1.4 **Управління доступом до даних та їх інтегрованість.**

У сучасному цифровому світі дані стали одним з найцінніших активів. Їх обсяг постійно зростає, а різноманітність джерел та форматів ускладнює завдання управління доступом та забезпечення їхньої інтегрованості. Ефективне управління доступом є ключовим для забезпечення безпеки даних, дотримання нормативних вимог та оптимізації бізнес-процесів.

Що таке управління доступом до даних?

Управління доступом до даних (УДД) – це сукупність заходів, спрямованих на визначення того, які користувачі мають доступ до яких даних та які дії вони можуть з ними виконувати. Цей процес передбачає:

- Ідентифікацію та аутентифікацію: Визначення особи користувача та перевірка його достовірності.
- Авторизацію: Надання користувачу певних прав доступу до даних та систем.
- Облік: Відстеження дій користувачів з даними.
- Контроль доступу: Запобігання несанкціонованому доступу до даних.

Інтегрованість даних

Інтегрованість даних – це процес об’єднання даних з різних джерел в єдине логічне ціле. Це дозволяє отримувати більш повну та достовірну інформацію для прийняття рішень.

Зв’язок між УДД та інтегрованістю даних

УДД та інтегрованість даних тісно пов’язані між собою. З одного боку, інтеграція даних створює нові виклики для УДД, оскільки збільшується кількість даних та джерел, що потребують захисту. З іншого боку, ефективне УДД є необхідною умовою для успішної інтеграції даних, оскільки дозволяє контролювати доступ до об’єднаних даних та запобігати несанкціонованому їх використанню.

Виклики управління доступом до даних та їх інтегрованості

- Різноманітність систем та даних: Сучасні організації використовують різноманітні системи та зберігають дані в різних форматах, що ускладнює управління доступом.
- Зростання кількості даних: Великі обсяги даних ускладнюють їх захист та управління доступом.
- Віддалений доступ: Збільшення кількості віддалених працівників підвищує ризики несанкціонованого доступу.
- Хмарні технології: Перехід до хмарних обчислень створює нові виклики для забезпечення безпеки даних.
- Регуляторні вимоги: Дотримання нормативних вимог щодо захисту даних, таких як GDPR, вимагає впровадження складних механізмів управління доступом.

Для ефективного управління доступом до даних та їх інтегрованості необхідно:

- Впровадження систем управління доступом: Використання спеціалізованого програмного забезпечення для управління правами доступу.
- Інтеграція систем: Об’єднання різних систем в єдину інформаційну систему для забезпечення єдиного підходу до управління доступом.
- Класифікація даних: Розподіл даних на категорії за рівнем конфіденційності та доступності.
- Регулярний аудит: Проведення регулярних аудитів систем безпеки для виявлення вразливостей.

- Навчання персоналу: Проведення навчань для співробітників щодо правил безпеки та управління доступом.
- Двофакторна аутентифікація: Використання додаткових засобів аутентифікації для підвищення рівня безпеки.
- Шифрування даних: Захист даних за допомогою криптографічних методів.

Управління доступом до даних та їх інтегрованість є важливими аспектами забезпечення безпеки інформації в організації. Ефективне вирішення цих завдань дозволяє підвищити рівень захисту даних, дотриматися нормативних вимог та оптимізувати бізнес-процеси.

### 1.5 **Стандарти та регулювання в галузі цифрової трансформації обліку.**

Цифрова трансформація обліку кардинально змінила підходи до ведення бухгалтерського обліку. З одного боку, це відкрило нові можливості для автоматизації процесів, підвищення ефективності та точності обліку. З іншого боку, виникла необхідність у розробці нових стандартів та регулятивних норм, які б забезпечили надійність, достовірність та порівнянність фінансової звітності в умовах цифрової трансформації.

Чому необхідні стандарти та регулювання?

- Забезпечення порівнянності: Стандарти дозволяють порівнювати фінансову звітності різних компаній, що є важливим для інвесторів, кредиторів та інших користувачів фінансової інформації.
- Підвищення довіри: Дотримання стандартів сприяє підвищенню довіри до фінансової звітності.
- Зменшення ризиків: Стандарти та регулювання допомагають мінімізувати ризики помилок та шахрайства в обліку.
- Спрощення міжнародної торгівлі: Спільні стандарти полегшують ведення бізнесу на міжнародному рівні.

Основні стандарти та регулювання в галузі цифрової трансформації обліку

- Міжнародні стандарти фінансової звітності (МСФЗ): МСФЗ є основним набором стандартів для складання фінансової звітності. Хоча вони не містять конкретних вимог щодо використання певних технологій, МСФЗ визначають принципи, яких слід дотримуватися при складанні фінансової звітності в цифровому форматі.
- Загальний регламент про захист даних (GDPR): GDPR встановлює високі стандарти захисту персональних даних, які також стосуються облікових систем. Компанії, що використовують цифрові технології в обліку, повинні забезпечити конфіденційність та безпеку персональних даних.
- Стандарти контролю внутрішньої звітності (COSO): COSO розробляє рамки для оцінки та покращення систем контролю внутрішньої звітності. Ці рамки можуть бути адаптовані для систем обліку, які використовують цифрові технології.
- Національні стандарти та регулювання: Кожна країна має свої національні стандарти та регулювання в галузі бухгалтерського обліку, які можуть доповнювати або уточнювати міжнародні стандарти.

Основні виклики та напрямки розвитку

- Цифрова трансформація аудиту: Аудитори повинні адаптуватися до нових технологій та розробити нові методи аудиту цифрових систем обліку.
- Захист даних: Забезпечення безпеки даних в умовах цифрової трансформації є одним з найважливіших завдань.
- Штучний інтелект: Використання штучного інтелекту в обліку створює нові можливості, але також вимагає розробки нових стандартів та регулятивних норм.
- Блокчейн: Технологія блокчейн може революціонізувати облік, але її використання потребує розробки спеціальних стандартів.

Перспективи розвитку

- Посилення ролі даних: Дані стануть ще більш цінним активом, а їх управління та аналіз стануть ключовими компетенціями для бухгалтерів.
- Автоматизація рутинних задач: Штучний інтелект та машинне навчання дозволять автоматизувати багато рутинних задач в обліку, що звільнить час для аналізу та прийняття рішень.
- Розвиток хмарних технологій: Хмарні технології нададуть нові можливості для зберігання та обробки даних, а також для співпраці між різними учасниками облікового процесу.
- Збільшення прозорості: Цифрова трансформація сприятиме підвищенню прозорості фінансової звітності.

Стандарти та регулювання в галузі цифрової трансформації обліку відіграють важливу роль у забезпеченні надійності, достовірності та порівнянності фінансової звітності. З розвитком технологій виникають нові виклики, які потребують розробки нових стандартів та адаптації існуючих. Бухгалтери та аудитори повинні постійно вдосконалювати свої знання та навички, щоб ефективно працювати в умовах цифрової трансформації.

## Контрольні запитання

1. Чому необхідні стандарти та регулювання в галузі цифрової трансформації обліку?
2. Які основні міжнародні стандарти застосовуються в обліку?
3. Як GDPR впливає на ведення обліку?
4. Які виклики виникають при аудиті систем обліку, що використовують цифрові технології?
5. Які переваги та ризики пов’язані з використанням штучного інтелекту в обліку?
6. Як блокчейн може змінити облік?
7. Які основні принципи захисту персональних даних визначені в GDPR?
8. Як відрізняється законодавство США щодо захисту персональних даних від GDPR?
9. Які виклики виникають при забезпеченні захисту персональних даних у глобалізованому світі?

10. Які основні принципи захисту персональних даних визначені в GDPR?
11. Як відрізняється законодавство США щодо захисту персональних даних від GDPR?
12. Які виклики виникають при забезпеченні захисту персональних даних у глобалізованому світі?