ЛАБОРАТОРНА РОБОТА № 1

Підготував Вавринович Михайло ПМІ-43

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

1.

Букмекерська контора – це організація, яка приймає ставки на різноманітні спортивні події та інші події з метою грошового обороту на ставках.
Управлінська структура букмекерської контори:

- **Вище керівництво:**
    - **Генеральний директор:** Основний виконавчий орган, відповідає за стратегічне керівництво та прийняття стратегічних рішень.
    - **Рада директорів:** Група висококваліфікованих і досвідчених осіб, які надають поради та наглядають за діяльністю компанії.
- **Фінансовий відділ:**
    - **Фінансовий директор:** Відповідає за фінансовий план, бюджетування та фінансовий звіт.
    - **Бухгалтерія:** Здійснює облік фінансових операцій та підготовку фінансових звітів.
- **Оперативний відділ:**
    - **Директор з оперативної діяльності:** Відповідає за щоденне управління букмекерською діяльністю, встановлення коефіцієнтів, обробку ставок та виплати виграшів.
    - **Аналітики:** Займаються аналізом спортивних подій та статистичними даними для визначення коефіцієнтів.

- **Маркетинг і реклама:**
    - **Менеджер з маркетингу:** Відповідає за розробку та реалізацію маркетингових стратегій та рекламних кампаній.
    - **PR-менеджер**: Займається відносинами з громадськістю та управлінням іміджем компанії.
- **ІТ-відділ:**
    - **Директор з інформаційних технологій**: Забезпечує правильне функціонування онлайн-платформи, безпеку даних та розвиток нових технологій.
- **Клієнтський сервіс:**
    - **Менеджери з обслуговування клієнтів:** Відповідають за вирішення питань і проблем клієнтів та надають консультації.
- **Юридичний відділ:**
    - **Юрист:** Здійснює правовий моніторинг, готує договори та вирішує правові питання.

2.

Стратегічний рівень:

На стратегічному рівні букмекерська контора визначає основні цілі та напрямки свого розвитку на довгострокову перспективу. Деякі аспекти цього рівня включають:

- **Глобальна стратегія:** Вирішення питань, таких як географічний охоплення, цільова аудиторія, розширення продуктової лінійки тощо.
- **Фінансове планування:** Визначення бюджетів, інвестиційних стратегій та фінансових цілей.
- **Ризик-менеджмент:** Оцінка та управління ризиками, пов'язаними зі змінами в законодавстві, конкурентним середовищем та іншими факторами.

Тактичний рівень:

На тактичному рівні приймаються рішення та формулюються плани, які допомагають досягти стратегічних цілей. Основні аспекти тактичного рівня для букмекерської контори можуть включати:

- **Кампанії та маркетингові заходи:** Визначення рекламних стратегій, бонусних програм, просування бренду.
- **Створення нових продуктів:** Розробка нових ставок, покращення інтерфейсу користувача, запуск мобільних додатків.
- **Аналіз конкурентів:** Слідкування за стратегіями конкурентів і прийняття заходів для збереження чи здобуття конкурентних переваг.

Операційний рівень:

Операційний рівень включає в себе щоденне керівництво та виконавчу діяльність. Деякі ключові аспекти операційного рівня для букмекерської контори:

- **Керування коефіцієнтами:** Встановлення та оновлення коефіцієнтів для ставок в режимі реального часу відповідно до змін в спортивних подіях.
- **Обробка ставок і виплати:** Забезпечення ефективної обробки ставок та вчасних виплат виграшів.
- **Контроль за ігровим процесом:** Моніторинг спортивних подій та результатів для вирішення ставок.
- **Клієнтський сервіс:** Вирішення питань клієнтів, надання інформації та допомоги.

Взаємодія між цими рівнями дозволяє букмекерській конторі ефективно реалізовувати свою стратегію, виконувати тактичні завдання та забезпечувати безперервну операційну діяльність.

3.

Апаратне забезпечення:

1. **Сервери та ДЦ (дата-центр):** Букмекерська контора використовує потужні сервери для забезпечення безперервності операцій, зберігання великої кількості даних та обчислень у реальному часі. Дата-центр забезпечує надійне розміщення серверного обладнання та забезпечення його безперебійної роботи.
2. **Робочі станції та термінали:** Для співробітників, що працюють в офісі, використовуються робочі станції, термінали або персональні комп'ютери для доступу до інформаційних систем та виконання офісних завдань.
3. **Мережеве обладнання:** Використовуються комутатори, маршрутизатори та інше мережеве обладнання для побудови локальної комп'ютерної мережі та забезпечення доступу до глобальної мережі Інтернет.

Системне програмне забезпечення:

1. **Операційні системи:** Сервери можуть використовувати операційні системи, такі як Linux або Windows Server, а робочі станції – Windows або macOS.
2. **Бази даних:** Для зберігання та обробки великого обсягу інформації використовуються бази даних, наприклад, MySQL, PostgreSQL або Oracle.
3. **Антивірусне програмне забезпечення:** Забезпечує захист від вірусів, шкідливих програм та інших загроз безпеці.

Мережева інфраструктура:

1. **Локальна комп'ютерна мережа (LAN):** Забезпечує внутрішнє з'єднання між робочими станціями та серверами в офісі. Використовуються комутатори для передачі даних внутрішньої мережі.
2. **Доступ до Інтернету:** Мережеві пристрої, такі як маршрутизатори, забезпечують доступ до Інтернету для робочих станцій та серверів.

3. **Захист мережі:** Використовуються засоби безпеки, такі як брандмауери та VPN, для захисту від несанкціонованого доступу та збереження конфіденційності даних.

Автоматизовані інформаційні системи управління:

1. **Система прийому ставок:** Автоматизована система для прийому ставок в режимі реального часу, врахування коефіцієнтів та обробки інформації про результати спортивних подій.
2. **Фінансова система**: Автоматизована система для ведення фінансового обліку, бюджетування та формування фінансових звітів.
3. **Система аналітики та прогнозування**: Використовується для аналізу спортивних подій, визначення тенденцій та формування коефіцієнтів.
4. **Система клієнтського сервісу:** Для ведення бази клієнтів, обробки запитань та ведення історії взаємодії з клієнтами.

Аналіз стану інформатизації:

1. **Переваги:** Покращення швидкості та точності прийому ставок, оптимізація фінансового управління, підвищення ефективності аналітики та прогнозування.
2. **Виклики:** Забезпечення безпеки даних та фінансових транзакцій, постійне оновлення та підтримка програмного та апаратного забезпечення, забезпечення стабільності мережі та доступності сервісів.

4.

Місця зберігання інформації:

1. **Сервери та ДЦ**: Основні дані та бази даних.
2. **Робочі станції**: Інформація працівників та проектів.
3. **Хмарні сервіси**: Зберігання для гнучкості та доступу.
4. **Архіви**: Фізичні та електронні архіви для старих даних.

Засоби захисту інформації:

1. **Аутентифікація та авторизація**: Сильні паролі та 2FA.
2. **Шифрування Даних**: Захист від несанкціонованого доступу.
3. **Резервне Копіювання**: Запобігання втратам даних.
4. **Фізична Безпека**: Контроль доступу та відеоспостереження.
5. **Системи виявлення та запобігання вторгнень**: Моніторинг та блокування підозрілих дій.
6. **Оновлення та Патчі**: Регулярне оновлення ПЗ та виправлення вразливостей.
7. **Навчання та Свідомість персоналу**: Едукація з кібербезпеки та усвідомленість ризиків.

5. Доступність:

- *Оцінка:* Вища
- *Пояснення:* Букмекерські контори зазвичай надають доступ до своїх інформаційних ресурсів широкому колу користувачів. Вони забезпечують доступність веб-сайту, мобільних додатків і інших каналів для зручного користування клієнтів.

Цілісність

- *Оцінка:* Середня
- *Пояснення:* Цілісність інформаційних ресурсів може бути вплинута факторами, такими як оновлення коефіцієнтів, результати подій тощо. Зазвичай букмекери прагнуть підтримувати точність інформації, але можливі помилки або зміни через зовнішні обставини.

Конфіденційність

- *Оцінка:* Висока

- *Пояснення:* Букмекери віддають велике значення захисту конфіденційної інформації користувачів, такої як особисті дані та фінансова інформація. Вони застосовують шифрування та інші технічні заходи безпеки для забезпечення конфіденційності клієнтів.

Аналіз результатів оцінювання:

- Букмекерська контора демонструє високий рівень доступності, що сприяє комфортному користуванню сервісами.
- Цілісність інформації в середньому рівні, оскільки можливі зміни коефіцієнтів та інших даних у зв'язку з подіями.
- Конфіденційність забезпечена на високому рівні, що важливо для збереження довіри клієнтів.

Цілком можливо, що конкретні обставини можуть вплинути на ці оцінки. Важливо зазначити, що букмекери повинні вдосконалювати свої системи безпеки та інформаційні ресурси, оскільки ці аспекти завжди в еволюції через нові технології та загрози.

6.

1. Правовий захист інформації:

- Закони та стандарти: Підприємство повинно підпорядковуватись Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та іншим відповідним законодавством. Слід також дотримуватись стандартів і методик, зокрема "Помаранчевої книги" для класифікації інформаційних систем.
- Напрямки захисту ІБ: Забезпечення конфіденційності, цілісності та доступності інформації, враховуючи специфіку галузі. Реалізація заходів для виконання вимог законів та стандартів.

2. Організаційний захист інформації:

- Заходи на організаційному рівні: Розробка та впровадження політик безпеки, навчання персоналу, контроль за доступом, визначення правил заохочення та покарання за порушення інформаційної безпеки.
- Структура служби безпеки: Створення служби безпеки, яка відповідає структурі підприємства та специфіці його діяльності, з оцінкою ризиків та використанням політики безпеки.

3. Інженерно-технічний захист інформації:

- Територія та пересування персоналу: Впровадження систем відеоспостереження, контроль за доступом, використання технічних засобів автентифікації.
- Технічні засоби захисту: Встановлення систем відеоспостереження, пожежної сигналізації, автентифікації з магнітними картками та інші засоби безпеки.

4. Програмно-технічний захист інформації:

- Програмні рішення: Використання антивірусного контролю, шифрування даних, системи автентифікації та інших заходів відповідно до політики безпеки.

Оцінка ризиків:

- Аналіз ризиків: Оцінка ризиків повинна враховувати можливі загрози, вразливості та можливі наслідки порушень безпеки. Для цього використовуються стандартні методи оцінки ризиків.

Висновки:

- Ці заходи враховують вимоги законодавства та специфіку підприємства.
- Система організаційного та технічного захисту покликана забезпечити повноту захисту інформації від різних загроз.

- Регулярне оновлення та перевірка систем забезпечить актуальність та ефективність заходів безпеки на підприємстві.

Цей комплексний підхід дозволяє підприємству максимально ефективно захищати свою інформацію від різних видів загроз.