

Волинський національний університет імені Лесі Українки
Факультет економіки та управління
Кафедра економіки і торгівлі

Олена Павлова, Костянтин Павлов, Анна Мохнюк, Олександр Шабала

РИЗИКИ В ОРГАНІЗАЦІЇ ДІЯЛЬНОСТІ ЕЛЕКТРОННОГО БІЗНЕСУ
Методичні рекомендації до практичних занять
та виконання самостійної роботи

Луцьк – 2025

УДК 330.342.146:330.16(07)
П 12

*Рекомендовано до друку науково-методичною радою Волинського
національного університету імені Лесі Українки
(протокол № 3 від 19 листопада 2025р.)*

Рецензенти:

Садовська І.Б., д.е.н., професор, завідувач кафедри обліку і оподаткування Волинського національного університету імені Лесі Українки.

Павлова О.М., Павлов К.В., Мохнюк А.М., Шабала О.П.

Я45 Методичні рекомендації до практичних занять та виконання самостійної роботи з освітнього компонента «Ризики в організації діяльності електронного бізнесу» для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 076 Підприємництво та торгівля освітньо-професійної програми Підприємництво, торгівля та біржова діяльність денної форми навчання / уклад. Павлова О.М., Павлов К.В., Мохнюк А.М., Шабала О.П. Луцьк: ВНУ ім. Лесі Українки, 2025. 81 с.

Методичні рекомендації до практичних занять та виконання самостійної роботи з освітнього компонента «Ризики в організації діяльності електронного бізнесу» для здобувачів освіти другого (магістерського) рівня вищої освіти за спеціальністю 076 Підприємництво та торгівля, освітньо-професійної програми Підприємництво, торгівля та біржова діяльність денної форми навчання містять основні вимоги до виконання практичних завдань та самостійної роботи.

Рекомендовано здобувачам другого (магістерського) рівня вищої освіти денної форми навчання за спеціальністю 076 Підприємництво та торгівля.

УДК 378.2:001.891(072) Я45
© Павлова О. М., Павлов К.В.,
Мохнюк А.М., Шабала О.П.
© Волинський національний
університет імені Лесі Українки, 2025

ЗМІСТ

Вступ.....	
1. Мета і завдання виконання практичних занять із освітнього компонента «Ризики в організації діяльності електронного бізнесу».....	
2. Тематика практичних занять.....	
Тема 1. Кіберзагрози та захист даних в е-комерції.....	
Тема 2. Фінансові ризики електронного бізнесу	
Тема 3. Операційні ризики онлайн-платформ	
Тема 4. Правові та регуляторні ризики	
Тема 5. Репутаційні ризики в цифровому середовищі	
Тема 6. Ризики конфіденційності та безпеки клієнтських даних	
Тема 7. Технологічні ризики при впровадженні інновацій	
Тема 8. Ризики, пов'язані з логістикою та доставкою	
Тема 9. Соціальні ризики та вплив на споживача	
Тема 10. Конкурентні ризики в електронному бізнесі.....	
Тема 11. Ризики інтелектуальної власності	
Тема 12. Управління ризиками в міжнародному електронному бізнесі	
Тема 13. Ризики, пов'язані з шахрайством та недобросовісною конкуренцією	
Тема 14. Ризики масштабування та зростання електронного бізнесу	
3. Тематика самостійної роботи.....	
4. Перелік тем для написання рефератів.....	
5. Оцінювання знань студентів.....	
6. Розподіл балів за формами контролю.....	
7. Перелік джерел рекомендованої літератури.....	

ВСТУП

Освітній компонент "Ризики в організації діяльності електронного бізнесу" розроблено так, щоб надати здобувачам вищої освіти необхідні знання для формування сучасного системного мислення та комплексу спеціальних умінь, практичних навичок у галузі підприємництва та торгівлі. Це дозволить їм глибоко розуміти особливості функціонування електронних бізнес-моделей та процесів, а також ефективно ідентифікувати, аналізувати та керувати ризиками, що виникають у зазначеній сфері.

Таким чином в курсі представлено як огляд теоретичних основ виникнення ризиків, методів їх оцінки, так і практичні аспекти управління ризиками в електронній комерції, кібербезпеці, захисті даних та інвестиційних проєктах електронного бізнесу.

1.МЕТА І ЗАВДАННЯ ВИКОНАННЯ ПРАКТИЧНИХ ЗАНЯТЬ

Мета дисципліни – надання здобувачам вищої освіти комплексного розуміння природи ризиків, що притаманні цій сфері. Курс покликаний сформувати практичні навички для ідентифікації, аналізу та оцінки ризиків, а також розробки ефективних стратегій управління ними. Це забезпечить стабільність і безпеку бізнес-процесів у цифровому середовищі.

Завдання курсу:

Розвиток у студентів здатності застосовувати отримані знання в практичних ситуаціях. Це включає вміння діяти відповідально та свідомо, взаємодіяти з учасниками ринку, займатися бізнес-плануванням та оцінювати кон'юнктуру ринків з урахуванням усіх можливих ризиків.

Інтегральна компетентність (ІК)

Здатність визначати та розв'язувати складні економічні задачі та проблеми, приймати відповідні аналітичні та управлінські рішення у сфері підприємництва, торгівлі та біржової діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій за невизначених умов та вимог.

Загальні компетенції

ЗК 2. Вміння виявляти, ставити та вирішувати проблеми.

ЗК 4. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

Фахові компетенції

СК 2. Здатність проводити оцінювання продукції, товарів і послуг в підприємницькій та торговельній діяльності.

СК 3. Здатність до ефективного управління діяльністю суб'єктів господарювання в сфері підприємництва та торгівлі.

Програмні результати навчання

РН 2. Визначати, аналізувати проблеми підприємництва, торгівлі і біржової діяльності та розробляти заходи щодо їх вирішення.

РН 4. Застосовувати бізнес-комунікації для підтримки взаємодії з представниками різних професійних груп.

РН 9. Розробляти і приймати рішення, спрямовані на забезпечення ефективності діяльності суб'єктів господарювання у сфері підприємницької та торговельної діяльності.

РН 10. Вирішувати проблемні питання, що виникають в діяльності підприємницьких та торговельних структур за умов невизначеності та ризиків.

2. ТЕМАТИКА ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1. Кіберзагрози та захист даних в е-комерції.

Мета: ознайомити студентів із розкриттям основних ризиків, пов'язаних із кіберзагрозами в електронному бізнесі, а також вивчення методів захисту даних, що забезпечують безпеку функціонування онлайн-платформ і довіру клієнтів.

Кіберзагрози є одними з найнебезпечніших факторів для електронного бізнесу, оскільки саме цифрове середовище є ключовим майданчиком для здійснення операцій, обробки замовлень, проведення платежів та зберігання персональних даних користувачів. Будь-яка втрата або витік інформації може призвести до значних фінансових збитків, втрати клієнтів та серйозного підризу репутації. Однією з найпоширеніших кіберзагроз залишаються хакерські атаки, які можуть набувати різних форм: від простого злому акаунтів користувачів до складних багаторівневих атак на сервери компаній. Метою таких дій є отримання несанкціонованого доступу до фінансової та персональної інформації, крадіжка коштів або шантаж із вимогою викупу.

Захист даних в електронній комерції базується на комплексному підході. Одним із найважливіших інструментів є впровадження багатофакторної автентифікації, яка ускладнює доступ до акаунтів навіть у випадку, коли пароль став відомим третім особам. Значну роль відіграє також шифрування даних, що передаються між користувачем і сервером, адже воно

унеможливиює перехоплення інформації у відкритому вигляді. Резервне копіювання є ще одним обов'язковим елементом, адже дозволяє швидко відновити дані у випадку злomu чи технічного збою.

Організації електронного бізнесу мають приділяти особливу увагу не лише технічним, а й організаційним заходам. Важливим аспектом є регулярне оновлення програмного забезпечення, навчання персоналу основам кібергігієни та створення внутрішніх правил щодо роботи з конфіденційною інформацією. Саме поєднання сучасних технологічних рішень та відповідальної поведінки співробітників формує ефективну систему захисту.

Хакерські атаки є одним із найпоширеніших і найнебезпечніших ризиків для будь-якого електронного бізнесу. Їхня мета полягає у несанкціонованому доступі до внутрішніх систем компанії, баз даних клієнтів або фінансових ресурсів. Хакери можуть використовувати різноманітні методи — від брутфорсу паролів і використання шкідливого програмного забезпечення до складних DDoS-атак, які паралізують роботу вебсайту або платформи. Результатом подібних дій є не лише прямі фінансові втрати, але й пошкодження репутації бізнесу, оскільки клієнти починають сумніватися у його надійності. Особливу небезпеку становлять сучасні форми атак, які здійснюються цілими організованими групами та мають на меті довгострокове проникнення у систему. У такому разі компанія може протягом тривалого часу навіть не здогадуватися, що всі її дані поступово контролюються сторонніми особами.

Фішинг ґрунтується на маніпуляціях із довірою користувачів. Шахраї створюють електронні листи, повідомлення в месенджерах або вебсторінки, які виглядають ідентично офіційним ресурсам банків, поштових служб чи самого бізнесу. Людина, яка не помітила підробку, добровільно надає свої паролі, дані банківських карток чи іншу конфіденційну інформацію. Для електронної комерції фішинг має подвійний негативний ефект. По-перше, страждають клієнти, які втрачають гроші та довіру. По-друге, шкодить

репутації компанії, оскільки навіть у випадку, коли сама платформа не була зламана, споживачі пов'язують негативний досвід саме з нею. Боротьба з фішингом вимагає як технічних рішень (системи виявлення підроблених сайтів і повідомлень), так і активної інформаційної кампанії серед клієнтів, аби вони знали, як виглядає справжнє листування від компанії.

Резервне копіювання є одним із найефективніших інструментів збереження даних у разі хакерських атак, збоїв обладнання чи людських помилок. Воно полягає у регулярному створенні дублікату всієї інформації на окремих серверах або хмарних сховищах. У разі знищення або пошкодження основної бази даних компанія може швидко відновити її з резервної копії, мінімізувавши втрати. Важливою умовою є те, щоб резервні копії зберігалися у зашифрованому вигляді й не були фізично пов'язані з головною системою, інакше атака може зачепити і їх. Ефективна політика резервного копіювання передбачає як щоденні автоматичні бекапи критичних даних, так і довгострокове зберігання попередніх версій, що дозволяє відкотитися до безпечного стану навіть після складних кібератак.

Шифрування виступає фундаментальним засобом захисту інформації в електронному бізнесі. Суть цього методу полягає у перетворенні даних у спеціальний код, який не може бути прочитаний без ключа розшифрування. Завдяки цьому навіть у випадку перехоплення інформації зловмисники не отримають жодної користі, адже всі відомості будуть представлені у вигляді незрозумілого набору символів. У практиці електронної комерції особливого значення набуває шифрування при передачі даних між клієнтом і сервером (протокол SSL/TLS), а також шифрування баз даних, у яких зберігаються фінансові та персональні відомості. Надійне шифрування є ознакою серйозного ставлення компанії до безпеки, і клієнти все частіше звертають увагу на наявність захищеного з'єднання перед тим, як здійснювати оплату онлайн.

Багатофакторна автентифікація (MFA) є сучасним і дієвим способом запобігання несанкціонованому доступу до облікових записів клієнтів та

внутрішніх систем компанії. Вона передбачає, що користувач для входу в акаунт має підтвердити свою особу кількома способами — наприклад, ввести пароль, отримати код у SMS або мобільному додатку, підтвердити вхід відбитком пальця чи скануванням обличчя. Це значно знижує ризик злому, адже навіть якщо зловмисники отримають пароль, їм усе одно бракуватиме додаткового підтвердження. Для бізнесу впровадження багатофакторної автентифікації є важливим кроком не лише у захисті клієнтів, а й у створенні атмосфери довіри, коли користувач відчуває, що його безпека є пріоритетом.

Додаткові аспекти:

- **Внутрішні загрози** – часто компанії фокусуються на зовнішніх хакерах, але не менш критичні ризики, що походять від співробітників: ненавмисне розголошення даних, неправильне поводження з конфіденційною інформацією, використання слабких паролів, підробка або видалення інформації.

- **Соціальна інженерія** – окрім фішингу, існують складніші методи маніпулювання працівниками чи клієнтами: смс-шахрайство (smishing), телефонні атаки (vishing), створення фейкових веб-сторінок або акаунтів для викрадення даних.

- **Атаки на сторонні сервіси та API** – сучасні платформи часто інтегровані з платіжними сервісами, CRM, маркетинговими системами. Недостатній контроль над API може стати джерелом витоку даних або дозволити несанкціонований доступ до критичних систем.

- **Резервування та відновлення після збоїв** – не просто резервне копіювання, а створення багаторівневих планів disaster recovery: локальні та хмарні копії, регулярне тестування відновлення даних, визначення критичних елементів бізнесу, які повинні працювати безперервно.

- **Моніторинг та аудит безпеки** – автоматизовані системи спостереження за активністю користувачів і внутрішніх процесів допомагають виявляти підозрілі дії на ранньому етапі. Логи, регулярний

аудит доступів та прав користувачів дозволяють швидко локалізувати інциденти.

- **Законодавчі аспекти кібербезпеки** – дотримання GDPR, локальних стандартів захисту даних, правил роботи з фінансовою інформацією, умови зберігання і обробки персональних даних, які можуть відрізнятися в різних країнах.

- **Освітні та превентивні заходи** – навчання співробітників щодо кібергігієни, регулярні тренінги з розпізнавання фішингових листів, симуляції атак для відпрацювання правильних дій у критичних ситуаціях.

- **Шифрування і захист каналів комунікації** – не лише для збереження даних у базі, але й для передавання інформації між сервером і користувачем, між підсистемами, а також резервних копій.

- **Управління доступом і ролями** – принцип мінімальних прав: співробітник отримує лише ті права, які потрібні для його роботи, регулярний перегляд доступів і контроль їх актуальності.

- **Психологічні аспекти безпеки користувачів** – створення політик безпечного користування акаунтами, інструкції щодо надійних паролів, двофакторної автентифікації, виявлення підозрілих повідомлень.

- **Взаємодія з партнерами та постачальниками** – кіберризики можуть походити з боку третіх осіб: підрядників, постачальників платіжних послуг, маркетингових агентств. Контроль контрактів і вимог до безпеки важливий для захисту екосистеми бізнесу.

- **Стрес-тести та сценарне моделювання атак** – оцінка готовності системи до DDoS-атак, пікових навантажень і складних комбінацій загроз. Це дозволяє виявити слабкі місця ще до реальної атаки.

- **Культура безпеки** – формування усвідомленого підходу до кібербезпеки у всіх співробітників, від керівництва до технічного персоналу. Це включає регулярне оновлення політик, інформаційні кампанії та винагороди за дотримання безпечних практик.

Питання для обговорення:

1. Принципи роботи систем багатофакторної автентифікації в електронній комерції
2. Основні міжнародні стандарти та протоколи шифрування даних (SSL, TLS, AES тощо)
3. Механізми організації резервного копіювання в хмарних сервісах
4. Види хакерських атак на онлайн-платформи та приклади їх реалізації
5. Методи запобігання фішинговим атакам на користувачів інтернет-магазинів
6. Практика впровадження політик безпеки персоналу в компаніях е-комерції
7. Роль системи моніторингу та виявлення вторгнень у захисті електронного бізнесу

Тема 2. Фінансові ризики електронного бізнесу.

Мета: ознайомити студентів з основними фінансовими ризиками, які супроводжують діяльність електронного бізнесу, а також розглянути шляхи їх виявлення, запобігання та мінімізації для забезпечення стабільності компанії на цифровому ринку.

Фінансові ризики в електронному бізнесі мають особливе значення, оскільки будь-які збитки або нестабільність у фінансових потоках безпосередньо впливають на розвиток, конкурентоспроможність та довіру з боку клієнтів і партнерів. Електронна комерція функціонує у швидкозмінному середовищі, де значна частина операцій проводиться онлайн, що створює додаткові можливості для шахрайських дій, технічних збоїв або валютних коливань. Основним завданням менеджменту є формування системи контролю та управління ризиками, яка дозволить передбачати потенційні проблеми й швидко реагувати на них.

Одним із найбільш поширених проявів фінансових ризиків є шахрайські транзакції. У процесі онлайн-оплати шахраї можуть використовувати вкрадені банківські картки, підроблені облікові записи чи незаконні способи підтвердження платежів. Такі дії призводять до втрати коштів як клієнтів, так і самої компанії, яка часто змушена компенсувати збитки постраждалим. Запобігти цьому допомагають системи моніторингу підозрілої активності, перевірка IP-адрес користувачів та впровадження додаткових етапів верифікації платежів.

Важливим фактором є нестабільність валютних курсів, що особливо актуально для компаній, які працюють на міжнародних ринках. Коливання валют може призвести до значних втрат у прибутку або додаткових витрат на конвертацію. Електронний бізнес змушений використовувати інструменти хеджування, проводити розрахунки у стабільніших валютах або заздалегідь планувати фінансові потоки з урахуванням можливих змін.

Ще одним різновидом ризику є проблеми ліквідності, коли компанія не має достатньо коштів для виконання поточних зобов'язань. Це може статися через затримку платежів від партнерів, збільшення витрат на логістику чи технічні послуги або ж через неправильне планування бюджету. Для зменшення цього ризику важливим є контроль над грошовими потоками, створення фінансових резервів та прогнозування доходів і витрат.

Кредитні ризики виникають у випадках, коли бізнес надає можливість відстроченої оплати клієнтам чи партнерам, але ті не виконують своїх зобов'язань. В електронній комерції це може стосуватися як B2B-сегменту (співпраця між компаніями), так і B2C (розстрочка або відкладені платежі для клієнтів). Для мінімізації таких ризиків застосовуються договори з чітко визначеними умовами, перевірка платоспроможності партнерів і страхування фінансових угод.

Окрему категорію становлять помилки в платіжних системах, які можуть призвести до подвійного списання коштів, затримки платежів або неправильного зарахування грошей. Подібні ситуації формують негативний

досвід у клієнтів і змушують компанію витрачати ресурси на виправлення проблем. Сучасні платіжні шлюзи прагнуть звести такі ризики до мінімуму шляхом регулярного тестування, сертифікації та використання захищених протоколів обробки транзакцій.

Фінансові ризики електронного бізнесу охоплюють широкий спектр проблем — від шахрайства та валютних коливань до технічних збоїв у платіжних системах. Для їх мінімізації компанії повинні формувати цілісну політику фінансової безпеки, яка базується на превентивних заходах, гнучкому управлінні ресурсами та впровадженні сучасних технологічних рішень.

Фінансові ризики електронного бізнесу можна класифікувати та розглядати за кількома напрямками.

1. **Кредитні та платіжні ризики** — це не лише неплатежі клієнтів, а й затримки від банків чи платіжних систем, проблеми з подвійним списанням та помилки при конвертації валют. Важливо відслідковувати такі моменти, щоб уникнути несподіваних фінансових втрат.

2. **Валютні ризики** — електронний бізнес, який працює на міжнародних ринках, піддається впливу коливань курсів валют. Без системи хеджування або фіксованих тарифів навіть невеликі зміни курсу можуть суттєво вплинути на прибуток.

3. **Ризики онлайн-платежів** — крім шахрайства з картками, існують спірні платежі (chargeback), некоректне використання купонів та бонусів, а також проблеми з інтеграцією платіжних сервісів.

4. **Цінові ризики** — різке коливання цін на товари або послуги може виникнути через агресивну конкуренцію, сезонні коливання попиту або нові податкові правила, що ускладнює прогнозування доходів.

5. **Зростання витрат при масштабуванні** — розширення бізнесу потребує додаткових інвестицій в ІТ-системи, логістику, маркетинг та персонал. Без контролю витрати можуть швидко перевищити бюджет і знизити прибутковість.

6. **Внутрішнє шахрайство та маніпуляції** – співробітники можуть ненавмисно або навмисно фальсифікувати дані, підробляти документи або проводити неправомірні транзакції, що створює додатковий фінансовий тиск.

7. **Податкові та регуляторні ризики** – несподівані зміни законодавства або штрафи за недотримання правил обліку можуть серйозно вплинути на бюджет і фінансові плани.

8. **Ліквідність та управління грошовими потоками** – ризик недостатньої грошової маси для покриття короткострокових зобов'язань особливо критичний у періоди пікового навантаження або сезонних коливань продажів.

9. **Інвестиційні ризики** – вкладення в нові технології, сервіси або ринки може не окупитися, що особливо небезпечно для стартапів і малого бізнесу в електронній комерції.

10. **Аналіз фінансових показників та прогнозування** – відсутність регулярного контролю за потоками коштів і порівняння з бюджетом призводить до непередбачуваних проблем і затримок у прийнятті рішень.

11. **Ризики партнерських відносин** – неплатоспроможність партнерів, затримки поставок або зміни умов контрактів можуть створити додатковий фінансовий тиск.

12. **Стрес-тести та сценарне моделювання** – перевірка фінансової стійкості бізнесу у «крайніх» ситуаціях (раптове падіння попиту, масові повернення товарів, збої у логістиці) дозволяє виявити слабкі місця та підготувати план дій.

13. **Резерви та страхування** – формування фінансових «подушок безпеки» і використання страхових продуктів для захисту від непередбачених витрат, кібератак або логістичних проблем.

Питання для обговорення:

1. Основні методи виявлення шахрайських транзакцій у системах електронної комерції

2. Механізми страхування фінансових операцій в онлайн-бізнесі
3. Використання інструментів хеджування для зниження валютних ризиків
4. Системи моніторингу та управління ліквідністю у цифрових компаніях
5. Технології запобігання помилкам у платіжних системах
6. Ризики, пов'язані з міжнародними фінансовими операціями, та методи їх мінімізації

Тема 3. Операційні ризики онлайн-платформ.

Мета: ознайомити студентів з основними операційними ризиками, що виникають у процесі функціонування онлайн-платформ, а також розглянути способи їх ідентифікації, попередження та подолання для забезпечення стабільної роботи електронного бізнесу.

Операційні ризики охоплюють усі внутрішні процеси компанії, пов'язані з управлінням платформою, обробкою замовлень, підтримкою клієнтів та технічним забезпеченням. Вони виникають як через людський фактор, так і через технічні несправності, що в сукупності можуть значно знизити ефективність бізнесу та рівень довіри користувачів. Для електронної комерції операційні ризики особливо небезпечні, оскільки від надійності та швидкості роботи платформи залежить безпосередньо клієнтський досвід.

Одним із ключових проявів операційних ризиків є збої в роботі онлайн-систем. Перевантаження серверів, технічні помилки програмного забезпечення або відсутність належної інфраструктури призводять до недоступності сайту чи мобільного додатку. У таких випадках бізнес втрачає замовлення, а клієнти можуть перейти до конкурентів. Запобігання таким проблемам передбачає використання масштабованих серверних рішень, регулярне тестування систем та застосування резервних потужностей.

Не менш важливим є ризик, пов'язаний із людськими помилками персоналу. Неправильне введення даних, некоректна обробка замовлень,

несвоєчасна відповідь клієнтам або порушення внутрішніх регламентів здатні спричинити фінансові втрати та зіпсувати репутацію компанії. Для мінімізації цих загроз бізнес впроваджує автоматизацію процесів, внутрішні стандарти роботи, системи навчання та регулярний контроль якості.

Особливу увагу слід приділити ризикам у сфері клієнтського обслуговування. Невчасна відповідь на звернення, низька якість підтримки або відсутність зворотного зв'язку формують негативне враження про компанію та знижують рівень лояльності клієнтів. Для вирішення цієї проблеми використовуються багатоканальні системи комунікації (чат-боти, телефонна підтримка, електронна пошта), а також моніторинг задоволеності клієнтів.

Важливим аспектом є також ризик логістичних збоїв, що напряду пов'язаний із виконанням замовлень. Затримки у доставці, помилки в комплектації товарів чи неправильне відображення статусу відправки на сайті створюють додаткові труднощі для споживачів. Онлайн-платформи повинні інтегрувати свої системи з надійними логістичними операторами та забезпечувати прозорий контроль усіх етапів доставки.

Ще один вид операційних ризиків пов'язаний із недостатньою безперервністю бізнес-процесів. Будь-які зовнішні фактори (відключення електроенергії, відсутність інтернет-з'єднання, збої у сторонніх сервісах) можуть паралізувати роботу компанії. Тому для електронного бізнесу важливим є створення планів безперервності діяльності (Business Continuity Plan), які дозволяють швидко відновити роботу після інциденту.

Таким чином, операційні ризики охоплюють усі аспекти щоденної діяльності електронного бізнесу та можуть проявлятися у вигляді технічних, організаційних і людських помилок. Своєчасне їх виявлення та системний підхід до управління дозволяють мінімізувати їх вплив, підвищити стабільність роботи платформи та зміцнити довіру з боку клієнтів.

Операційні ризики онлайн-платформ не обмежуються звичними збоями системи або людськими помилками. Існує ряд специфічних факторів, які можуть серйозно впливати на ефективність діяльності.

Наприклад, нестабільність сторонніх сервісів і API часто стає справжньою проблемою. Платформа може залежати від кількох зовнішніх постачальників одночасно, і будь-яка зміна їхніх інтерфейсів, оновлення або припинення підтримки здатні паралізувати обробку замовлень чи передачу даних.

Ще один виклик – оновлення та релізи системи. Навіть невелика помилка під час тестування або впровадження може спричинити падіння сервісу або некоректну роботу важливих функцій.

Також варто враховувати ризики складних ланцюгів постачання даних і контенту. Коли платформа залежить від кількох джерел інформації одночасно, збій на будь-якому рівні може призвести до затримок або втрати даних, що безпосередньо впливає на користувацький досвід.

Особливо небезпечні ризики масштабування. Під час раптового зростання активності користувачів вузькі місця в базах даних, недостатня ємність серверів або проблеми з балансуванням навантаження здатні суттєво знизити якість сервісу.

Не можна забувати і про людський фактор. Адміністратори, які неправильно налаштовують систему, співробітники, що ненавмисно видаляють дані, або новачки без належного навчання – усе це створює критичні ситуації, які складно передбачити звичайними заходами безпеки.

Питання для обговорення:

1. Основні підходи до управління безперервністю бізнес-процесів в електронній комерції
2. Методи запобігання технічним збоям у роботі онлайн-платформ
3. Роль автоматизації у зниженні ризику людських помилок

4. Інструменти контролю якості обслуговування клієнтів на онлайн-платформах
5. Особливості організації роботи служби підтримки у великих маркетплейсах
6. Впровадження внутрішніх регламентів та стандартів для мінімізації операційних ризиків

Тема 4. Правові та регуляторні ризики.

Мета: ознайомити студентів з основними правовими та регуляторними ризиками, які виникають у діяльності електронного бізнесу, а також розглянути можливі шляхи їх уникнення, мінімізації та подолання для забезпечення правової захищеності та стабільності функціонування компаній у цифровому середовищі.

1. Правові ризики в електронному бізнесі

Правові ризики становлять одну з найважливіших загроз для електронного бізнесу, оскільки вони пов'язані з прямим порушенням законодавства, що може мати наслідком фінансові втрати, судові позови, штрафи та навіть заборону діяльності. У сфері цифрової комерції правові проблеми виникають не тільки у відносинах між компаніями та клієнтами, а й у відносинах з державними органами, постачальниками та міжнародними партнерами.

Одним із ключових аспектів є порушення договірних зобов'язань. У традиційному бізнесі всі відносини чітко фіксуються у письмових договорах, однак в електронному середовищі багато транзакцій відбувається онлайн через оферти, електронні угоди або публічні пропозиції. Неправильно складений договір або відсутність юридично чітко визначених умов може призвести до конфліктів з клієнтами чи партнерами. Наприклад, відсутність чітких правил повернення товару або формулювань щодо відповідальності сторін може стати підставою для судових позовів.

Важливим блоком є порушення прав споживачів. У більшості країн діє законодавство, яке захищає права клієнтів при купівлі товарів чи послуг онлайн. Це стосується, зокрема, права на повернення товару, обміну продукції, відмови від підписки, прозорості цін та умов доставки. Якщо компанія не дотримується цих правил, вона може отримати штрафні санкції, втратити ліцензії або зіткнутися з масовими позовами від клієнтів. Для електронного бізнесу особливо важливо формувати чітку політику обслуговування та відкрито інформувати клієнтів про їхні права.

Окрему категорію становить недотримання вимог у сфері захисту персональних даних. Оскільки електронні компанії постійно збирають та зберігають персональну інформацію користувачів (імена, адреси, банківські дані), вони підпадають під дію законів про захист конфіденційності. У Європейському Союзі, наприклад, діє Загальний регламент із захисту даних (GDPR), а у США — власні стандарти захисту інформації. Недотримання цих вимог може обійтися бізнесу в мільйони доларів штрафів та завдати непоправної шкоди його репутації.

Серйозним джерелом проблем стає незаконне використання інтелектуальної власності. Онлайн-компанії нерідко використовують чужі торгові марки, контент, фотографії чи програмне забезпечення без належної ліцензії. Такі дії можуть спричинити судові позови від правовласників, вимогу компенсації збитків або навіть заборону діяльності на певних ринках. Це стосується як великих маркетплейсів, які зобов'язані контролювати законність товарів від сторонніх продавців, так і малих інтернет-магазинів, що використовують чужі зображення чи тексти.

Не менш актуальним є питання електронних договорів та підписів. У різних країнах існують різні правові режими, які визначають, чи має електронний підпис юридичну силу та за яких умов. Це створює труднощі для міжнародного електронного бізнесу, коли угоди укладаються між сторонами з різних юрисдикцій. У разі виникнення спору суд може не

визнати електронну угоду належним доказом, що створює серйозні правові ризики для компанії.

Ще один важливий блок — податкові ризики. В умовах електронної комерції компанії повинні сплачувати податки відповідно до законодавства тієї країни, де вони здійснюють діяльність. Однак у глобальній мережі складно визначити, де саме відбулася операція: у країні клієнта, у країні продавця чи на міжнародному рівні. Це створює ризик подвійного оподаткування або, навпаки, звинувачення у податковому шахрайстві. Крім того, регулярні зміни у податковому законодавстві вимагають від бізнесу постійного моніторингу та адаптації.

Додатково варто відзначити суперечки щодо юрисдикції. У міжнародному електронному бізнесі часто виникає питання: за законами якої держави вирішувати конфлікти. Якщо компанія зареєстрована в одній країні, клієнт знаходиться в іншій, а сервер розташований у третій, виникає юридична невизначеність. Такі ситуації потребують попереднього врегулювання у договорах або звернення до міжнародних арбітражних органів.

У підсумку правові ризики електронного бізнесу охоплюють широкий спектр проблем — від договірних відносин і захисту персональних даних до оподаткування та міжнародної юрисдикції. Їх недооцінка може призвести не лише до фінансових збитків, але й до повного припинення діяльності компанії на окремих ринках. Саме тому підприємствам у сфері електронної комерції необхідно забезпечувати юридичний супровід своєї діяльності, залучати професійних юристів та регулярно оновлювати політики відповідно до актуальних вимог законодавства.

1. Регуляторні ризики в електронному бізнесі

Регуляторні ризики виникають через недотримання вимог державних органів та нормативних актів, що регулюють діяльність електронного бізнесу, і можуть мати серйозні наслідки у вигляді штрафів, блокування сервісів або обмеження діяльності на певних ринках. У сучасному

цифровому середовищі регуляторні норми постійно змінюються, що створює додатковий виклик для компаній, які прагнуть залишатися легальними та конкурентоспроможними.

Одним із основних аспектів є регулювання електронної комерції. Це включає вимоги щодо реєстрації бізнесу, ліцензування певних видів діяльності, дотримання правил торгівлі товарами та послугами онлайн. Компанії зобов'язані дотримуватися встановлених правил розрахунку вартості, відображення податків, оформлення чеків та надання клієнтам інформації про товари. Недотримання таких правил може призвести до штрафів та адміністративних санкцій.

Важливу роль відіграє регулювання фінансових транзакцій. Електронні платежі та використання платіжних систем підпадають під контроль банківських і фінансових регуляторів. Бізнес повинен дотримуватися правил протидії відмиванню грошей (AML), знати свого клієнта (KYC) та забезпечувати прозорість фінансових операцій. Порушення цих норм загрожує не лише штрафами, але й блокуванням рахунків або втратами ліцензій на проведення платежів.

Регуляторні вимоги щодо захисту персональних даних також є ключовим джерелом ризиків. Законодавство різних країн (GDPR у ЄС, CCPA у США та національні закони в інших державах) передбачає суворі норми обробки та зберігання персональних даних користувачів. Компанії повинні впроваджувати внутрішні політики захисту даних, проводити аудит безпеки та забезпечувати можливість клієнтам контролювати свої дані. Ігнорування цих вимог призводить до великих штрафів і значного зниження довіри з боку користувачів.

Окремо слід виділити регуляторні норми у сфері реклами та маркетингу. Вони регламентують, яким чином компанії можуть просувати товари та послуги, використовувати персональні дані для таргетингу, робити email-розсилки або проводити промоакції. Порушення цих правил може

призвести до блокування рекламних кампаній, штрафів або заборони на використання певних каналів комунікації.

Також важливим є регулювання конкуренції та антимонопольні вимоги. Онлайн-платформи повинні дотримуватися правил чесної конкуренції, уникати недобросовісних практик, маніпуляцій цінами або обмеження доступу конкурентів. Недотримання антимонопольних норм може призвести до судових позовів, величезних штрафів і втрати довіри партнерів.

Ще одним джерелом регуляторних ризиків є міжнародне законодавство та транскордонне регулювання. Компанії, які працюють на декількох ринках, стикаються з різними стандартами безпеки, податковими режимами та вимогами до електронних угод. Це створює необхідність адаптації процесів під специфіку кожної юрисдикції та підтримки юридичного супроводу на глобальному рівні.

В цілому, регуляторні ризики електронного бізнесу охоплюють широкий спектр аспектів діяльності — від дотримання правил торгівлі та реклами до міжнародного законодавства і фінансового контролю. Їх систематичне управління, своєчасне оновлення внутрішніх політик та залучення юридичних експертів дозволяють компаніям працювати легально, мінімізувати фінансові та репутаційні втрати та забезпечити стабільний розвиток бізнесу.

Питання для обговорення:

1. Як правильно скласти електронні договори, щоб вони мали юридичну силу у різних юрисдикціях
2. Основні вимоги GDPR та методи їх впровадження в електронних платформах
3. Практичні способи забезпечення відповідності нормам захисту персональних даних у міжнародній діяльності

4. Особливості застосування електронного підпису у транскордонних угодах
5. Вплив податкових змін на операційну діяльність онлайн-бізнесу
6. Методи контролю дотримання антимонопольних та конкурентних правил на онлайн-платформах
7. Регулювання електронної комерції: основні вимоги щодо ліцензування та реєстрації бізнесу
8. Вимоги щодо реклами і маркетингу: як уникнути порушення правил просування товарів і послуг
9. Практики моніторингу та аудиту відповідності внутрішніх політик компанії регуляторним нормам
10. Юридичні ризики у випадку невиконання міжнародних контрактів та способи їх мінімізації

Тема 5. Репутаційні ризики в цифровому середовищі.

Мета: ознайомити студентів із природою репутаційних ризиків у сфері електронного бізнесу, показати їх вплив на діяльність компанії, клієнтську довіру та конкурентоспроможність, а також розглянути методи управління, моніторингу та мінімізації таких ризиків.

Репутаційні ризики — це загрози, пов'язані з втратою довіри клієнтів, партнерів чи громадськості до компанії внаслідок негативних подій або сприйняття її діяльності. У цифровому середовищі, де інформація поширюється миттєво і неконтрольовано, навіть незначний інцидент може швидко перерости у масштабну кризу, яка поставить під загрозу існування бізнесу.

Такі ризики можуть виникати через низьку якість обслуговування, невиконання зобов'язань перед клієнтами, публікацію негативних відгуків у соціальних мережах, витік даних користувачів або асоціацію бренду з етичними чи правовими порушеннями. Особливо небезпечною є ситуація,

коли проблеми не вирішуються вчасно, а компанія ігнорує суспільну реакцію.

Репутаційні ризики у сфері електронного бізнесу охоплюють не лише роботу з клієнтами, а й корпоративну культуру, прозорість бізнес-процесів та готовність компанії швидко реагувати на кризові ситуації у цифровому просторі.

1. Джерела репутаційних ризиків у цифровому середовищі

Одним із головних джерел репутаційних ризиків є негативний клієнтський досвід. Якщо покупець залишається незадоволеним якістю товару, затримкою доставки чи відсутністю підтримки, він часто публікує свій відгук у соціальних мережах або на спеціалізованих платформах. Негативна інформація поширюється значно швидше, ніж позитивна, і навіть кілька критичних коментарів здатні сформувати уявлення про ненадійність компанії.

Велику роль відіграє соціальний резонанс у медіа-просторі. У цифрову епоху будь-яка помилка чи скандал може перетворитися на інформаційний привід, що призведе до масштабного поширення негативу. Наприклад, помилка у рекламній кампанії, яка виявилася образливою для певної аудиторії, здатна викликати хвилю критики та бойкот продуктів.

Ще одним потужним фактором є витік або неналежний захист персональних даних. Якщо компанія стає жертвою кібератаки або недбало ставиться до конфіденційної інформації клієнтів, довіра до бренду падає миттєво. В умовах конкуренції користувачі віддають перевагу бізнесу, який гарантує безпеку їхніх даних.

Варто виділити і низький рівень прозорості бізнес-процесів. Якщо клієнти підозрюють компанію в приховуванні важливої інформації, маніпуляціях цінами чи введенні в оману щодо характеристик товарів, це швидко формує негативний імідж. Особливо небезпечною є ситуація, коли факт обману підтверджується, адже тоді відновити довіру стає надзвичайно складно.

До репутаційних ризиків належать також етичні та соціальні аспекти діяльності компанії. Сучасні споживачі звертають увагу на соціальну відповідальність бізнесу: екологічність виробництва, чесне ставлення до працівників, дотримання принципів рівності. Якщо компанія ігнорує ці фактори або потрапляє у скандал, пов'язаний із трудовою експлуатацією чи шкодою довкіллю, це значно підриває її репутацію.

Ще один вагомий фактор — недобросовісна конкуренція. Конкуренти можуть поширювати фейкові новини або негативний контент про компанію з метою зіпсувати її імідж. У такому випадку особливо важливими є моніторинг інформаційного поля та своєчасне реагування.

Важливим джерелом репутаційних ризиків є і некомпетентна реакція на кризу. Якщо компанія не відповідає на скарги клієнтів або заперечує очевидні проблеми, це лише поглиблює кризу. Затягування з комунікацією у цифровому просторі може перетворити локальну проблему на глобальну катастрофу для бренду.

2. Способи зниження репутаційних ризиків

Найпершим і найважливішим методом управління репутаційними ризиками є активний моніторинг цифрового середовища. Використання спеціалізованих інструментів для відстеження згадок бренду у соціальних мережах, блогах і медіа дозволяє компанії своєчасно виявляти потенційні загрози та реагувати на них ще на ранніх етапах.

Ефективним способом запобігання негативним наслідкам є впровадження чітких стандартів обслуговування клієнтів. Висока якість сервісу, швидке реагування на запити, ввічливість і готовність вирішувати проблеми формують позитивне враження та зменшують імовірність негативних відгуків.

Ключову роль відіграє прозорість і чесність у комунікації. Якщо виникає проблема, компанія повинна чесно визнати її, пояснити причини та представити план вирішення. Такий підхід допомагає зберегти довіру навіть у складних ситуаціях, адже клієнти цінують відкритість.

Важливим є і захист персональних даних клієнтів. Впровадження сучасних технологій шифрування, регулярний аудит систем безпеки та навчання персоналу допомагають запобігти витокам і зміцнюють репутацію компанії як надійного партнера.

Окрему увагу слід приділяти корпоративній соціальній відповідальності. Участь у соціальних, екологічних та благодійних ініціативах, прозора політика щодо співробітників і партнерів формують позитивний імідж бренду. У сучасному бізнес-середовищі соціально відповідальна компанія отримує більше лояльності від клієнтів.

Ще одним напрямом є підготовка планів кризового реагування. Компанія повинна мати напрацьовані сценарії дій у разі репутаційної кризи: визначену команду для комунікації, алгоритми швидкого реагування, готові меседжі для медіа. Це дозволяє оперативно взяти ситуацію під контроль та мінімізувати шкоду.

Крім того, компанія має активно працювати над створенням позитивного інформаційного поля. Публікація історій успіху клієнтів, відкритість до зворотного зв'язку, ведення корпоративних блогів і активна присутність у соціальних мережах формують позитивний образ бренду, що допомагає легше переживати навіть тимчасові труднощі.

У цифровому середовищі репутаційні ризики можуть посилюватися через невідповідність контенту і меседжів різним каналам комунікації. Наприклад, реклама або пости у соціальних мережах можуть по-різному сприйматися аудиторією Facebook, Instagram чи LinkedIn, і те, що на одному каналі виглядає нейтрально, на іншому може викликати негативну реакцію.

Велику роль відіграють внутрішні конфлікти і комунікація співробітників. Витоки інформації або публічні скандали за участю працівників, пости в особистих акаунтах або незгода з корпоративною політикою здатні швидко транслюватися у репутаційні втрати.

Не менш важливим є ризик втрати контролю над партнерськими зв'язками. Компанії, що співпрацюють із зовнішніми постачальниками,

маркетинговими агентствами чи логістичними операторами, ризикують, якщо партнери порушують етичні стандарти або допускають помилки, що відображаються на бренді.

Також варто враховувати ризики, пов'язані з впливом «вірусного контенту» та мемів, коли навіть невелика подія стає предметом ширшого обговорення у соціальних мережах. Неправильна інтерпретація дій компанії або її висловлювань може миттєво набрати популярності й завдати шкоди репутації.

Додатковим джерелом репутаційних ризиків є недооцінка негативного впливу автоматизованих систем і відгуків. Наприклад, бот-загрози, фейкові коментарі або низькоякісні оцінки сервісу на платформах відгуків здатні формувати у користувачів хибне враження про компанію, якщо їх не контролювати.

Ще один аспект – запізніла або некоректна реакція на критичні події в медіа. Навіть якщо компанія вчасно виявила проблему, неправильний тон комунікації або несвоєчасне реагування здатні значно погіршити ситуацію.

Крім того, сучасні репутаційні ризики тісно пов'язані з етичними алгоритмами і ШІ, що використовуються компанією. Наприклад, упереджені рекомендаційні системи, неправильне таргетування реклами або помилки в автоматизованих сервісах можуть сприйматися як дискримінаційні або недобросовісні, що шкодить іміджу.

Нарешті, варто розглянути ризики, пов'язані з глобальною присутністю бренду. Різні культурні та соціальні стандарти у країнах, де працює компанія, можуть впливати на сприйняття бренду і створювати непередбачувані репутаційні виклики.

Питання для обговорення:

1. Які інструменти моніторингу соціальних мереж є найбільш ефективними для відстеження репутаційних ризиків

2. Як правильно реагувати на негативний відгук клієнта, щоб він не переріс у масштабну кризу
3. Які стратегії варто застосовувати при поширенні фейкових новин про компанію
4. У чому різниця між репутаційними ризиками, пов'язаними з якістю продукту, і тими, що виникають через витік даних
5. Як можна використати кризову ситуацію для зміцнення бренду та довіри клієнтів
6. Чи повинна компанія офіційно коментувати всі конфліктні ситуації у ЗМІ та соціальних мережах
7. Які ключові принципи має містити план кризових комунікацій для цифрового бізнесу
8. Які приклади успішного подолання репутаційних криз у сфері електронного бізнесу можна вважати зразковими
9. Чи може корпоративна соціальна відповідальність реально знизити репутаційні ризики, чи це лише маркетинговий інструмент

Тема 6. Ризики конфіденційності та безпеки клієнтських даних.

Мета: ознайомити студентів із сутністю ризиків, що виникають у сфері збереження та обробки персональних даних клієнтів в електронному бізнесі, а також показати їх вплив на довіру користувачів та стабільність компанії.

1. Несанкціонований доступ

Несанкціонований доступ до клієнтських даних є однією з найпоширеніших загроз у сфері електронного бізнесу. Він може виникати через слабкі паролі, відсутність багатофакторної автентифікації, вразливості у програмному забезпеченні чи внутрішні зловживання співробітників. Отримавши доступ, зловмисники можуть викрадати персональну інформацію, здійснювати шахрайські транзакції чи змінювати дані клієнтів. Для запобігання цьому необхідно впроваджувати сучасні системи

автентифікації, контролю доступу, шифрування та проводити регулярний аудит безпеки.

2. Витоки персональної інформації

Витік персональних даних може відбутися як унаслідок кібератак, так і через людський фактор — недбалість співробітників, помилки при збереженні чи передачі інформації. Особливо небезпечними є витоки фінансових даних (номерів карток, CVV-кодів), адрес, телефонів та паролів користувачів. Втрата таких даних призводить до фінансових збитків для клієнтів і колосальних репутаційних втрат для компанії. Захист від витоків включає використання безпечних каналів зв'язку, систем шифрування, регулярне оновлення програмного забезпечення та контроль доступу до чутливої інформації.

3. Слабка політика збереження даних

Багато компаній стикаються з проблемою неправильної або застарілої політики збереження даних. Це може включати надмірне накопичення інформації, яка не використовується, зберігання даних без належного рівня захисту чи відсутність чітких правил їх видалення. Така слабка політика відкриває можливості для кібератак і ускладнює відповідність вимогам законодавства (наприклад, GDPR). Ефективна політика має передбачати принцип мінімізації даних (збір лише необхідної інформації), визначені терміни зберігання, регулярне видалення застарілих даних та аудит внутрішніх процедур.

4. Злом акаунтів

Злом акаунтів клієнтів або співробітників є поширеним способом доступу до конфіденційної інформації. Часто зловмисники використовують фішинг, атаки методом підбору паролів чи повторне використання паролів на різних сервісах. Наслідки злому можуть включати викрадення персональних і фінансових даних, несанкціоновані покупки чи навіть блокування облікових записів. Для мінімізації цього ризику важливо впроваджувати двофакторну

автентифікацію, вимоги до складності паролів, механізми виявлення підозрілої активності та системи швидкого відновлення доступу.

5. Порушення довіри

Навіть якщо витік даних чи кібератака не призвели до прямого фінансового збитку, сам факт порушення конфіденційності здатний зруйнувати довіру клієнтів. Користувачі очікують, що їхня інформація буде максимально захищена, а компанія несе відповідальність за її безпеку. Порушення довіри часто має довгострокові наслідки: зменшення клієнтської бази, відтік користувачів до конкурентів, падіння продажів і репутаційні втрати. Для відновлення довіри необхідні відкритість у комунікації, швидка реакція на інциденти, компенсаційні заходи для постраждалих клієнтів і демонстрація підвищеного рівня безпеки у майбутньому.

6. Додаткові аспекти ризиків конфіденційності та безпеки клієнтських даних

Окремим фактором ризику є використання сторонніх сервісів та постачальників. Часто електронний бізнес інтегрує платіжні системи, маркетингові інструменти чи хмарні сервіси, які також мають доступ до клієнтських даних. Якщо їх рівень безпеки недостатній, це автоматично створює загрозу для компанії, яка відповідає перед користувачами за захист інформації. Тому важливо проводити аудит постачальників та укладати угоди про конфіденційність (NDA).

Ще одним джерелом небезпеки виступає використання застарілих технологій та слабких алгоритмів шифрування. Наприклад, зберігання паролів у відкритому вигляді чи використання застарілих протоколів (HTTP замість HTTPS) може створити серйозні вразливості. Це підкреслює потребу в регулярному оновленні інфраструктури та використанні сучасних стандартів захисту.

Не менш важливим є навчання персоналу. Багато витоків стаються через помилки співробітників: відкриття фішингових листів, передача даних третім сторонам або неправильна конфігурація систем. Тому інформаційна

безпека повинна включати постійні тренінги, внутрішні політики та перевірки.

Нарешті, компанії повинні дбати не лише про технічний захист, а й про юридичні аспекти збереження даних. Недотримання вимог національних та міжнародних законів (GDPR, CCPA тощо) може призвести до великих штрафів. Водночас прозора політика щодо даних (privacy policy) допомагає формувати довіру та демонструє відповідальність бізнесу перед клієнтами.

7. Заходи реагування після інциденту

У разі виявлення витоку або загрози безпеці клієнтських даних ключовим завданням компанії є швидке реагування, яке включає комплекс технічних, організаційних та комунікаційних дій.

По-перше, необхідно локалізувати проблему, тобто ізолювати уражені системи, закрити вразливості та зупинити подальше поширення витоку. Це може включати відключення певних серверів, обмеження доступу до облікових записів чи зміну паролів користувачів.

По-друге, потрібно провести всебічний аналіз інциденту — виявити джерело атаки, масштаби витоку, типи даних, які були скомпрометовані, і потенційні наслідки для клієнтів. Для цього залучаються як внутрішні фахівці, так і зовнішні експерти з кібербезпеки.

Третім кроком є інформування постраждалих клієнтів. Важливо не приховувати факт інциденту, а повідомити користувачів про ситуацію, надати інструкції щодо зміни паролів, моніторингу фінансових операцій або блокування карток. Прозорість у комунікації допомагає мінімізувати втрату довіри.

Четвертим етапом є повідомлення регуляторних органів, якщо цього вимагає законодавство. Наприклад, згідно з GDPR, компанія зобов'язана протягом 72 годин повідомити про інцидент відповідні органи та клієнтів. Невиконання цього зобов'язання може призвести до значних штрафів.

Далі варто розробити і впровадити план відновлення систем — перевстановлення програмного забезпечення, додаткове шифрування,

впровадження нових механізмів автентифікації, аудит усіх підключених сервісів.

Останнім, але не менш важливим кроком є проведення внутрішнього аналізу та корекції політик безпеки, щоб уникнути повторення інциденту. Це включає оновлення протоколів, посилення контролю доступу, проведення тренінгів для персоналу, а також створення плану кризових дій на випадок нових загроз.

Ризики конфіденційності та безпеки клієнтських даних можна умовно поділити на три великі категорії: технічні, організаційні та юридичні.

1. Технічні ризики включають загрози, що виникають через вразливості програмного забезпечення, використання застарілих протоколів, слабе шифрування або помилки у налаштуванні систем. До цієї категорії належать несанкціонований доступ, злом акаунтів, витoki даних через кібератаки, а також відсутність багатофакторної автентифікації чи регулярного оновлення систем. Для зниження таких ризиків необхідно впроваджувати сучасні технічні рішення, шифрування, моніторинг безпеки та аудит інфраструктури.

2. Організаційні ризики пов'язані з внутрішньою політикою компанії, підготовкою персоналу та контролем за доступом до інформації. Слабка політика збереження даних, недотримання процедур обробки інформації, помилки співробітників і необізнаність щодо загроз підвищують ймовірність інцидентів. Мінімізувати ці ризики допомагають навчання працівників, чіткі внутрішні політики, розмежування прав доступу та постійний аудит процедур.

3. Юридичні ризики виникають при недотриманні вимог законодавства щодо захисту даних (наприклад, GDPR, CCPA) та при відсутності договорів з постачальниками на дотримання конфіденційності. Недотримання юридичних норм може призвести до великих штрафів та втрати довіри клієнтів. Для мінімізації цих ризиків компанія повинна

забезпечити відповідність законодавству, укласти NDA з партнерами та вести прозору політику обробки даних.

Такий підхід дозволяє чітко бачити, які аспекти потребують уваги, і створює основу для системного управління ризиками.

Питання для обговорення:

1. Які технічні та організаційні заходи найбільш ефективні для запобігання витокам даних у малому бізнесі
2. Як перевіряти надійність постачальників сторонніх сервісів, що мають доступ до клієнтських даних
3. Які приклади реальних витоків даних у відомих компаніях можна розглянути як навчальні кейси
4. Чи достатньо лише технічних рішень (шифрування, MFA) для захисту даних, чи ключовим є людський фактор
5. Як впливає прозора політика конфіденційності на рівень довіри клієнтів до електронного бізнесу
6. Які кроки має зробити компанія після інциденту витоку даних, щоб мінімізувати репутаційні та фінансові втрати

Тема 7. Технологічні ризики при впровадженні інновацій.

Мета: ознайомити студентів з особливостями виникнення технологічних ризиків у процесі впровадження інновацій в електронному бізнесі, розкрити їх основні види, причини появи та можливі наслідки для організацій, а також окреслити шляхи їхнього мінімізації.

У сучасному електронному бізнесі технологічні інновації є ключовим фактором конкурентоспроможності. Компанії постійно впроваджують нові цифрові рішення: хмарні сервіси, системи автоматизації, штучний інтелект, блокчейн-технології, мобільні додатки, big data-аналітику. Водночас, впровадження інновацій супроводжується ризиками технологічного

характеру, які можуть поставити під загрозу стабільність бізнес-процесів, фінансові результати та безпеку клієнтів.

Ці ризики зумовлені як технічними аспектами, так і людським фактором. З одного боку, нові технології можуть мати приховані вразливості, несумісність із наявною інфраструктурою чи нестачу тестування перед масштабним запуском. З іншого боку, персонал може бути недостатньо підготовлений до роботи з новими системами, що призводить до помилок у їх експлуатації.

Причини виникнення технологічних ризиків:

1. **Недостатнє тестування нових рішень** – компанії часто впроваджують інновації у прискореному режимі, щоб випередити конкурентів, ігноруючи етапи повноцінного тестування. Це створює ризики збоїв у роботі систем.

2. **Несумісність із наявною IT-інфраструктурою** – інтеграція нових технологій може вимагати повної перебудови внутрішніх процесів і програмного забезпечення, що тягне додаткові витрати і можливі збої.

3. **Швидке моральне старіння інновацій** – у цифровому середовищі технології швидко застарівають, і інвестиції, зроблені у впровадження певної системи, можуть втратити актуальність через 2–3 роки.

4. **Кіберзагрози та вразливості** – нові технології часто стають мішенню хакерів, адже виробники ще не встигли усунути всі слабкі місця. Наприклад, у перших версіях інноваційних платформ виявляються критичні недоліки захисту.

5. **Низька кваліфікація персоналу** – працівники не завжди встигають адаптуватися до нових систем, що створює ризик неправильного використання інструментів або порушення безпеки.

6. **Висока вартість впровадження та невизначений результат** – технологічні інновації потребують значних фінансових ресурсів, але не завжди гарантують очікуваний рівень ефективності.

Наслідки технологічних ризиків

Виникнення технологічних ризиків може мати широкий спектр негативних наслідків. Це тимчасові або довготривалі перебої у роботі платформи, втрата клієнтів через поганий користувацький досвід, фінансові збитки від простоїв чи помилкових транзакцій. Особливо небезпечним є ризик компрометації безпеки даних – при впровадженні нових технологій можуть відкриватися "дірки" у захисті, через які зловмисники отримують доступ до інформації клієнтів.

Ще одним наслідком є погіршення репутації компанії. Якщо клієнти стикаються з технічними збоями, повільною роботою сервісу чи втратами даних, вони швидко втрачають довіру і переходять до конкурентів.

Додатково, невдале впровадження інновацій може призвести до надмірних витрат: компанія інвестує значні кошти у проєкт, але він не приносить очікуваного результату, що підриває фінансову стабільність бізнесу.

1. Важливість управління технологічними ризиками

Сучасний електронний бізнес не може уникнути інновацій, адже відмова від їх впровадження означає втрату конкурентоспроможності. Тому управління технологічними ризиками є не просто опцією, а обов'язковим елементом стратегічного планування.

Компанії повинні створювати системи моніторингу й контролю ризиків, розробляти стратегії поступового впровадження нових технологій (поетапне тестування, пілотні проєкти, резервні рішення), проводити навчання персоналу, укладати контракти з постачальниками програмних продуктів, що передбачають гарантії технічної підтримки та оновлень.

Таким чином, успішне впровадження інновацій можливе лише тоді, коли компанія не лише прагне технологічних переваг, але й усвідомлює ризики, пов'язані з ними, та завчасно формує механізми їх подолання.

2. Технічні збої та нестабільність систем

Одним із найпоширеніших ризиків є технічні збої, що виникають через недостатнє тестування інноваційних продуктів або їхню несумісність з існуючою інфраструктурою. Непередбачені помилки у роботі програмного забезпечення можуть призвести до зависання систем, уповільнення транзакцій чи навіть повної зупинки електронної платформи. Це особливо критично для бізнесів, які працюють у режимі 24/7, адже навіть кілька хвилин простою можуть обернутися суттєвими фінансовими втратами та зниженням рівня довіри клієнтів.

3. Кіберзагрози та вразливості

Інноваційні технології, особливо на ранніх етапах свого розвитку, часто мають невиявлені вразливості. Хакери активно шукають слабкі місця у нових системах, оскільки вони зазвичай ще не мають відпрацьованих механізмів захисту. Наприклад, використання блокчейн-рішень чи штучного інтелекту може створювати нові вектори атак, про які компанія навіть не здогадувалася. Несвоєчасне оновлення або відсутність патчів робить системи ще більш уразливими.

4. Людський фактор та низька кваліфікація персоналу

Будь-які технологічні інновації потребують навчання та адаптації персоналу. Якщо компанія не інвестує в підвищення кваліфікації працівників, це створює ризик неправильного використання нових систем, виникнення помилок у роботі чи навіть випадкових витоків даних. Людський фактор залишається одним із головних джерел ризиків, оскільки навіть найсучасніша система безпеки може бути зруйнована необережними діями співробітників.

5. Фінансові ризики інновацій

Впровадження нових технологій завжди пов'язане зі значними витратами: закупівля обладнання, ліцензій, навчання персоналу, модернізація інфраструктури. Проте очікуваний економічний ефект не завжди досягається. Невдалі інноваційні проекти можуть призвести до втрати інвестицій, необхідності повторного впровадження іншого рішення або зниження

прибутковості компанії. Додатково варто враховувати ризик швидкого морального старіння технології: інновація, яка сьогодні є проривною, завтра може стати застарілою.

6. Проблеми інтеграції та сумісності

Нова система може не поєднуватися з існуючими бізнес-процесами або програмним забезпеченням. Це вимагає дорогих доробок, оновлення інфраструктури чи навіть повного переходу на нову платформу. Якщо інтеграція проходить невдало, компанія може стикнутися з подвійною проблемою — витраченими коштами та непрацюючими бізнес-процесами.

7. Ризик залежності від постачальників технологій

Багато інноваційних рішень постачаються сторонніми компаніями, і бізнес стає залежним від їхньої технічної підтримки, оновлень та цінової політики. Якщо постачальник збанкрутує, змінить умови ліцензування чи припинить підтримку продукту, компанія може залишитися з недієздатною системою без можливості її самостійної модернізації.

8. Репутаційні ризики від впровадження невдалих інновацій

Будь-яка інновація, яка не виправдала очікувань, негативно позначається на іміджі компанії. Клієнти сприймають збої в роботі сервісу, помилки в транзакціях чи незручний інтерфейс як ознаку непрофесійності. Це знижує рівень довіри, а у сфері електронного бізнесу довіра клієнтів є критично важливою.

Додаткові аспекти технологічних ризиків при впровадженні інновацій:

1. Ризики масштабованості та навантаження

Впровадження нових технологій може створити несподівані проблеми при збільшенні кількості користувачів або обсягу транзакцій. Наприклад, хмарна платформа чи система автоматизації може працювати без збоїв на етапі пілотного запуску, але під час масового використання виникають затримки, зависання або відмови сервісу. Цей аспект часто ігнорується на ранніх стадіях проєкту, проте він критично впливає на користувацький досвід та фінансові результати.

2. Ризики сумісності з майбутніми технологіями

Інновації не лише мають інтегруватися з наявною інфраструктурою, але й повинні бути гнучкими для подальшого розвитку. Якщо система не передбачає можливості масштабування або інтеграції з новими технологіями, компанія ризикує зіткнутися з високими витратами на повну заміну рішень у короткостроковій перспективі.

Ризики управління даними та аналітики

Багато інновацій передбачають активне використання великих обсягів даних. Неправильне налаштування потоків даних, некоректна обробка або відсутність контролю якості інформації можуть призвести до хибних бізнес-рішень. Наприклад, аналітика на основі некоректних даних може впливати на маркетингові кампанії, прогнозування продажів або стратегію розвитку продукту.

Ризики крос-функціональної взаємодії

Впровадження нових технологій часто зачіпає кілька відділів одночасно: ІТ, маркетинг, фінанси, логістику. Недостатня координація між командами може створити конфлікти, дублювання дій або пропуск критично важливих етапів. Такі ризики потребують належного планування, комунікації та визначення відповідальності за кожну фазу проєкту.

Ризики психологічної та культурної адаптації персоналу

Крім технічної підготовки, впровадження інновацій часто стикається з опором співробітників. Люди можуть сприймати нові процеси як загрозу власній роботі, що знижує ефективність використання систем і призводить до помилок. Управління цим ризиком потребує не лише навчання, а й побудови культури інновацій та мотивації персоналу.

Ризики етичного та соціального характеру

Інновації, особливо пов'язані з обробкою персональних даних, штучним інтелектом чи автоматизацією, можуть викликати суспільні чи регуляторні запитання. Неправильне використання алгоритмів або

порушення етичних стандартів здатне створити додаткові юридичні та репутаційні проблеми, навіть якщо технологія технічно працює правильно.

Ризики відсутності плану відкату та резервування

Нерідко компанії впроваджують інновації без продуманого плану відновлення старої системи у разі невдачі або без належних резервних рішень. Це збільшує вразливість бізнесу та ускладнює швидке реагування на непередбачені ситуації.

Питання для обговорення:

1. Які фактори найбільше впливають на ймовірність технічних збоїв під час впровадження нових технологій?
2. Чому інноваційні рішення особливо вразливі до кіберзагроз на початкових етапах використання?
3. Чи можна вважати недостатню підготовку персоналу основним джерелом технологічних ризиків, і чому?
4. Які методи оцінки ефективності інновацій застосовуються в електронному бізнесі для мінімізації фінансових втрат?
5. Проблема сумісності: як визначити, чи нова технологія буде інтегрована в існуючу інфраструктуру без суттєвих ускладнень?
6. Які ризики виникають у разі надмірної залежності бізнесу від одного постачальника технологій?
7. Як можна виміряти ймовірність швидкого морального старіння інноваційної технології?
8. Чи варто компанії впроваджувати експериментальні інновації, ризикуючи частиною репутації, чи краще чекати на стабільні рішення?
9. Як приклади з реальних кейсів (наприклад, збої в роботі великих онлайн-сервісів) демонструють наслідки невдалого впровадження інновацій?
10. Яку роль у зменшенні технологічних ризиків відіграє стратегія поступового впровадження (пілотні проекти, тестування на обмежених групах користувачів)?

Тема 8. Ризики, пов'язані з логістикою та доставкою.

Мета: ознайомити студентів з особливостями виникнення логістичних ризиків у електронному бізнесі, розкрити їх основні види, причини появи та можливі наслідки для організацій, а також окреслити шляхи мінімізації втрат у процесі доставки товарів та послуг.

Логістика та доставка є критично важливими складовими електронного бізнесу, оскільки швидкість, надійність і якість доставки безпосередньо впливають на рівень задоволеності клієнтів і репутацію компанії. Разом з тим, цей процес супроводжується численними ризиками, які можуть негативно впливати на фінансові результати, довіру споживачів та ефективність бізнесу.

Логістичні ризики можна поділити на кілька основних категорій: ризики, пов'язані з транспортуванням, зберіганням, управлінням запасами, організацією процесів і людським фактором. Кожен із цих напрямів має власні специфічні загрози, які потребують окремого аналізу та управління.

Основні типи ризиків:

1. Ризики

транспортування

Сюди входять затримки у доставці через погодні умови, транспортні аварії, поломки транспортних засобів, пробки або обмеження руху. Також можливі проблеми з логістичними операторами — ненадійні перевізники, помилки у маршрутах, відсутність страхування вантажу. Затримки транспортування негативно впливають на задоволеність клієнтів і можуть призвести до повернень або скасування замовлень.

2. Ризики

зберігання

та

складування

Вони пов'язані з неналежними умовами зберігання товарів, перевищенням термінів зберігання, пошкодженням або псуванням продукції, неправильною організацією складу та відсутністю систем контролю запасів. Особливо критичними є ризики для продуктів із обмеженим терміном придатності або високою чутливістю до температури та вологості.

3. Ризики управління запасами

Неправильне планування, відсутність автоматизованих систем обліку, помилки в прогнозуванні попиту або надмірні запаси можуть призвести до дефіциту товарів, простоїв у доставці, або навпаки — надлишку, який потребує додаткових витрат на зберігання чи утилізацію.

4. Ризики людського фактору

Помилки співробітників, недостатня кваліфікація, неправильне пакування або відправка товарів, недотримання стандартів безпеки — усе це створює ризики втрати або пошкодження вантажу. Крім того, внутрішні шахрайства, розкрадання або зловживання можуть стати джерелом фінансових і репутаційних втрат.

5. Ризики, пов'язані з третіми сторонами

Електронний бізнес часто використовує послуги сторонніх логістичних операторів або кур'єрських служб. Недотримання ними стандартів доставки, ненадійність або затримки стають прямим ризиком для компанії. Відсутність чітких договорів і SLA (Service Level Agreement) погіршує контроль і підвищує вірогідність конфліктів із клієнтами.

6. Ризики зовнішнього середовища

Погодні умови, природні катастрофи, політичні обмеження, страйки або проблеми на митниці можуть спричинити затримки у доставці та збільшення витрат. Ці ризики важко передбачити, але їх можна частково мінімізувати через планування альтернативних маршрутів і страхування вантажів.

7. Фінансові та економічні ризики

Коливання цін на паливо, транспортні тарифи, митні збори або зміни в законодавстві можуть збільшити вартість доставки. Також важливо враховувати ризики валютних коливань, якщо компанія працює на міжнародному ринку.

8. Репутаційні наслідки логістичних проблем

Збої в доставці безпосередньо впливають на довіру клієнтів. Затримки, пошкоджені товари або невідповідність термінів доставки призводять до

негативних відгуків, зниження повторних покупок і підриву конкурентних переваг компанії.

Для мінімізації ризиків, пов'язаних із логістикою та доставкою, компанії перш за все використовують сучасні технології планування і моніторингу. Оптимізація маршрутів, GPS-трекінг, автоматизовані платформи управління складом і аналітика дозволяють скоротити час доставки, уникнути затримок та надмірних витрат, а також контролювати залишки товарів, прогнозувати дефіцит або надлишок і своєчасно поповнювати запаси.

Важливим аспектом є робота з перевізниками та страхування вантажів. Використання резервних постачальників і кур'єрів забезпечує безперервність доставки навіть у разі відмови основного партнера. Страхування матеріальних цінностей під час транспортування та зберігання дозволяє мінімізувати фінансові втрати у випадку пошкодження, крадіжки або втрати товарів, особливо при міжнародних перевезеннях.

Не менш значущим є людський фактор і стандартизація процесів. Регулярне навчання персоналу складів і кур'єрів, інструктаж щодо безпечного поводження з товарами та контроль якості роботи допомагають зменшити помилки, пов'язані з людським фактором. Стандартизоване пакування з урахуванням чутливості товарів, вагових обмежень та температурного режиму знижує ймовірність пошкоджень, втрат і повернень.

Для підвищення ефективності важливе застосування сценарного планування і прозорості комунікації з клієнтами. Розробка альтернативних планів дій на випадок затримок, аварій або стихійних лих дозволяє швидко реагувати та мінімізувати наслідки. Регулярне інформування клієнтів про статус доставки, терміни та можливі затримки допомагає зберегти довіру навіть у разі непередбачуваних проблем.

Крім того, сучасний підхід включає етичні та екологічні аспекти. Оптимізація маршрутів з урахуванням енергозбереження, відповідальне ставлення до персоналу та дотримання екологічних стандартів не лише

знижує ризики репутаційних втрат, але й підвищує лояльність клієнтів та конкурентоспроможність компанії.

Логістика має багатовікову історію, і багато сучасних ризиків — це лише нові прояви старих проблем. Ще у середньовіччі торгівля вимагала організації перевезення товарів на великі відстані: каравани, річкові та морські шляхи. Торговці стикалися з ризиками розкрадання вантажу, нападів піратів, затримок через погодні умови, хвороби тварин-перевізників чи порушення політичної стабільності на маршруті. Втрата товару могла призвести до банкрутства або повного зникнення торгової точки.

У XVII–XIX століттях розвиток морських і залізничних перевезень відкрив нові можливості, але і нові ризики: поломки локомотивів, аварії на судах, неправильно складені вантажі, нестача стандартів пакування та страхування. Наприклад, у 1850-х роках поширеною проблемою було псування продуктів під час транспортування на великі відстані через відсутність холодильників і захищених складів.

Історія також демонструє важливість управління запасами та планування маршрутів: торгові компанії, які впроваджували централізовані склади та контроль над поставками, мали значно менші втрати. Досвід минулого показує, що ефективне управління логістикою завжди поєднує технічні, організаційні та людські аспекти, що й актуально для сучасного електронного бізнесу.

Сучасні технології — GPS-трекінг, автоматизовані склади, системи прогнозування попиту — лише цифрово вирішують ті ж самі класичні проблеми: затримки, втрати, пошкодження товарів, ненадійність партнерів і нестабільність зовнішніх умов. Історичний досвід підкреслює, що ризики логістики завжди існували, а сучасні рішення зменшують їх масштаби та підвищують надійність доставки.

Питання для обговорення:

1. Які фактори найбільше впливають на затримки у доставці товарів в електронному бізнесі?
2. Як неправильне прогнозування попиту може створювати логістичні ризики?
3. Чи можна зменшити ризики пошкодження товарів за допомогою покращеного пакування та стандартизації?
4. Яким чином погодні умови і природні катастрофи змінюють логістичні стратегії компаній?
5. Як впливає залежність від сторонніх перевізників на контроль за якістю доставки?
6. У яких випадках швидка доставка може призвести до негативних наслідків для бізнесу (економічних, репутаційних)?
7. Які інструменти прогнозування та аналітики допомагають мінімізувати логістичні ризики?
8. Як можна поєднати маркетингові обіцянки щодо доставки з реальними можливостями логістики?
9. Яким чином повернення та обмін товарів ускладнюють логістичний процес і створюють додаткові ризики?

Тема 9. Соціальні ризики та вплив на споживача.

Мета: ознайомити студентів із сутністю соціальних ризиків у сфері електронного бізнесу, показати, як вони впливають на взаємодію компанії зі споживачами, а також розкрити причини їх виникнення та можливі наслідки для бізнесу.

Соціальні ризики в електронному бізнесі виникають через складність взаємодії між компанією і суспільством або окремими групами споживачів. Вони можуть проявлятися у формі негативної реакції клієнтів, критики в медіа чи соцмережах, а також у втраті довіри до бренду через неетичну поведінку компанії, недотримання обіцянок або порушення стандартів

обслуговування. Такі ризики часто пов'язані з тим, що бізнес функціонує у відкритому цифровому середовищі, де інформація про діяльність компанії швидко поширюється і кожна помилка може мати масштабний ефект.

Соціальні ризики можуть виникати через неповну або некоректну комунікацію, відсутність прозорості у роботі, порушення соціальних або культурних норм, а також недостатнє врахування очікувань і потреб цільової аудиторії. Вони здатні впливати на репутацію компанії, формувати негативне сприйняття продуктів чи послуг і навіть знижувати обсяг продажів.

Особливу роль у соціальних ризиках відіграє поведінка споживачів у цифровому середовищі. Соціальні платформи, форуми та відгуки на сайтах створюють механізми швидкого поширення інформації про компанію, що робить негативні оцінки потенційно дуже шкідливими. Водночас такі ризики стимулюють бізнес постійно удосконалювати взаємодію зі споживачами, підвищувати якість обслуговування та прозорість діяльності.

Соціальні ризики також мають тенденцію до кумулятивного ефекту: один непомітний на перший погляд інцидент може спровокувати серію негативних реакцій, що ускладнює управління репутацією та вимагає стратегічного підходу до комунікації, управління конфліктами та запобігання кризовим ситуаціям. Врахування соціальних ризиків є невід'ємною складовою стратегічного планування та розвитку електронного бізнесу в сучасних умовах.

Негативні відгуки, критика та поширення негативної інформації про компанію у соціальних мережах, форумах або платформах для відгуків є одним із найпоширеніших соціальних ризиків в електронному бізнесі. Вони можуть виникати через різні причини: невчасну доставку, пошкоджений товар, некоректне обслуговування, непорозуміння щодо умов повернення, технічні збої на сайті, неточності у описі продукту або навіть через дії конкурентів, які поширюють неправдиву інформацію з метою дискредитації.

Такий ризик характеризується високою швидкістю поширення та потенційним масштабом: один незадоволений клієнт може залучити увагу

сотень або тисяч інших користувачів, що створює ефект «снігової кулі». Негативна інформація здатна швидко впливати на репутацію компанії, знижувати довіру до бренду та скорочувати обсяги продажів. Особливо чутливими є молодші аудиторії та активні користувачі соціальних мереж, для яких рекомендації та відгуки інших користувачів є ключовим фактором при прийнятті рішення про покупку.

Цей ризик також пов'язаний із психологічними аспектами поведінки споживачів. Люди більше схильні залишати відгуки, коли їхній досвід був негативним, ніж позитивним. Крім того, емоційний характер негативних коментарів і їхня публічність можуть призводити до формування стійкого негативного іміджу бренду, навіть якщо проблема була локальною або одноразовою.

Важливим чинником є відсутність швидкої та ефективної реакції компанії на критику. Якщо відгуки залишаються без відповіді, або реакція компанії виглядає формальною, це лише підсилює соціальний ризик і може призвести до додаткових негативних оцінок. У той же час стратегічна робота з коментарями — оперативна відповідь, пояснення ситуації, пропозиція компенсації або альтернативних рішень — здатна не лише мінімізувати шкоду, а й перетворити негативний досвід на позитивний іміджевий кейс.

Ще одним аспектом цього ризику є ефект вірусності у медіа-середовищі. Скріншоти, меми або відео з негативним контекстом можуть швидко поширюватися, виходячи за межі цільової аудиторії компанії, і навіть залучати увагу журналістів чи блогерів. Це створює необхідність постійного моніторингу соціальних платформ і готовності до кризових ситуацій у будь-який момент.

Щоб ефективно управляти цим ризиком, компанії застосовують комплекс заходів: моніторинг відгуків і згадок про бренд у реальному часі, активне ведення соціальних мереж, створення системи швидкого реагування на скарги, аналітику причин негативу, навчання персоналу правильної комунікації з клієнтами, а також превентивні дії — наприклад, чітка

інформація про товар, умови доставки та повернення, прозорі правила обслуговування.

Таким чином, негативний вплив від споживачів та соціальних платформ — це багатогранний соціальний ризик, який поєднує психологічні, комунікаційні та технологічні фактори. Його наслідки можуть бути швидкими і масштабними, але при системному підході до моніторингу та взаємодії з аудиторією цей ризик можна ефективно мінімізувати та перетворити у джерело навчання та підвищення лояльності клієнтів.

Ще одним важливим соціальним ризиком є недовіра до онлайн-покупок. Вона виникає через страх перед шахрайством, зломом банківських даних, неправдивими описами товарів або низькою якістю обслуговування. Клієнти, які сумніваються у безпечності сайту або надійності продавця, можуть відмовитися від покупки або шукати альтернативні сервіси, навіть якщо компанія пропонує конкурентні ціни. Недовіра також формується під впливом попереднього негативного досвіду або порад знайомих, тому її подолання вимагає системної роботи: прозорих правил, сертифікацій безпеки, гарантій та оперативної підтримки клієнтів.

Ще один аспект — зростання вимог клієнтів. Сучасні споживачі очікують швидкої доставки, високої якості обслуговування, простоти повернення товару та персоналізованих пропозицій. Якщо компанія не здатна відповідати цим очікуванням, це створює соціальний ризик: клієнти залишають негативні відгуки, знижують рівень лояльності і можуть перейти до конкурентів. Цей ризик особливо актуальний під час пікових періодів продажів або акцій, коли високий попит створює додаткові навантаження на логістику та підтримку клієнтів.

Культурні бар'єри та відмінності у соціальних нормах є ще одним джерелом соціальних ризиків у міжнародному електронному бізнесі. Наприклад, способи комунікації, оформлення рекламних матеріалів, колірна символіка або формулювання пропозицій можуть по-різному сприйматися у різних країнах. Ігнорування таких особливостей може призвести до

негативного сприйняття бренду, втрати довіри та зниження продажів на певних ринках.

Важливу роль відіграє також вплив соціальних мереж. Активність користувачів у Facebook, Instagram, TikTok та інших платформах здатна як підсилювати позитивний імідж компанії, так і створювати масштабні негативні ефекти. Поширення критики, мемів або вірусних скарг може миттєво поширитися на широку аудиторію, формуючи уявлення про бренд навіть у тих, хто раніше не був клієнтом. Соціальні мережі підсилюють ефект швидкого розповсюдження інформації, що робить необхідним постійний моніторинг і готовність до кризового реагування.

Ще одним ризиком є недостатня обізнаність споживачів щодо прав і правил онлайн-покупок. Часто користувачі не знають, як працює система повернення, гарантії або захисту даних, що призводить до конфліктів і скарг. Такі ситуації можуть впливати на репутацію компанії, навіть якщо вона діє у межах закону і стандартів обслуговування.

Соціальні ризики в електронному бізнесі є багатовимірними і включають як негативний вплив від клієнтів і соціальних платформ, так і недовіру до онлайн-покупок, зростання вимог клієнтів, культурні бар'єри та низьку обізнаність споживачів. Ефективне управління цими ризиками потребує комплексного підходу: прозорості комунікації, адаптації до культурних та регіональних особливостей, моніторингу соцмереж і постійного покращення сервісу та взаємодії з клієнтами.

Моделі та принципи управління соціальними ризиками:

1. Модель "PRAISE" для аналізу соціальних ризиків

Ця англомовна аббревіатура охоплює ключові напрями:

- **P** – Perception (сприйняття споживачами діяльності компанії);
- **R** – Reputation (репутаційні наслідки негативних ситуацій);
- **A** – Awareness (рівень обізнаності користувачів щодо продукту та сервісу);
- **I** – Influence (вплив соціальних мереж і медіа);

- **S – Sensitivity** (чутливість аудиторії до помилок або недоліків);
- **E – Engagement** (ефективність взаємодії з клієнтами і реагування на критику).

Використання цієї моделі дозволяє системно оцінювати потенційні ризики і планувати превентивні заходи.

2. Принцип превентивної комунікації

Соціальні ризики часто виникають через неповну або некоректну інформацію. Превентивна комунікація передбачає:

- своєчасне інформування про можливі зміни, проблеми чи затримки;
- прозорість щодо умов доставки, повернення товару та гарантій;
- регулярну взаємодію з аудиторією у соціальних мережах для підтримки довіри.

3. Модель зворотного зв'язку та реагування (Feedback Loop)

Вона передбачає постійний моніторинг відгуків і негайну реакцію на негатив:

- збір та аналіз коментарів і скарг у реальному часі;
- швидке вирішення проблем і надання компенсацій, якщо це доцільно;
- трансформація негативного досвіду клієнта у позитивний кейс для покращення іміджу бренду.

4. Принцип культурної адаптації

Для міжнародного бізнесу важливо враховувати культурні особливості аудиторії:

- адаптація рекламних повідомлень і сервісних матеріалів до локальних норм та традицій;
- уникання символіки або формулювань, що можуть бути сприйняті негативно;
- навчання персоналу специфіці спілкування з різними групами клієнтів.

5. Модель ризиків недовіри (Trust Risk Model)

Вона фокусується на факторах, що формують довіру або недовіру:

- безпека платежів і персональних даних;
- достовірність інформації про товари;
- відповідність обіцянок і реального сервісу;
- швидкість і якість реакції на проблеми клієнтів.

Ця модель допомагає прогнозувати, які дії компанії можуть зменшити або, навпаки, посилити соціальні ризики.

Питання для обговорення:

1. Які фактори найбільше спричиняють негативну реакцію споживачів у соціальних мережах?
2. Аналіз прикладів криз у соціальних мережах через негативні відгуки та визначення причин їх виникнення
3. Оцінка ефективності систем швидкого реагування компаній на скарги клієнтів
4. Як культурні бар'єри впливають на міжнародні маркетингові кампанії та комунікацію?
5. Моделювання сценаріїв соціальних ризиків: наслідки і варіанти реагування на критику
6. Розробка практичних рекомендацій для компаній щодо мінімізації соціальних ризиків та підвищення лояльності клієнтів
7. Які інструменти можна використовувати для моніторингу соціальних платформ і попередження репутаційних проблем?
8. Вивчення впливу недостатньої обізнаності споживачів про права та правила онлайн-покупок
9. Приклади ситуацій, коли компанії перетворювали негативні відгуки на позитивний іміджевий ефект
10. Як можна навчити персонал правильно взаємодіяти з клієнтами у кризових ситуаціях?

11. Оцінка ризиків, пов'язаних із вірусним поширенням негативної інформації у соцмережах

Тема 10. Конкурентні ризики в електронному бізнесі.

Мета: ознайомити студентів із сутністю конкурентних ризиків у електронному бізнесі, їхніми джерелами та впливом на діяльність компанії, а також розглянути стратегії управління цими ризиками для збереження конкурентних переваг.

Конкурентні ризики в електронному бізнесі виникають через постійну зміну ринку, швидкий розвиток технологій та глобальну доступність цифрових платформ. Вони проявляються у формі зростання конкуренції, тиску на ціни, зменшення частки ринку, втрати лояльності клієнтів та зниження прибутковості. Основними джерелами цих ризиків є дії конкурентів, зміни споживчих уподобань, поява нових технологій, а також доступність інформації, що дозволяє конкурентам швидко реагувати на стратегії компанії.

Електронний бізнес особливо чутливий до конкурентних ризиків через відкритість інформації, простоту виходу на ринок і низькі бар'єри входу для нових учасників. Зміни у поведінці конкурентів можуть впливати на швидкість адаптації компанії, її маркетингові кампанії, цінову політику та інноваційні рішення. Підприємства повинні постійно аналізувати ринок, слідкувати за трендами та впроваджувати стратегії диференціації продукту, щоб залишатися конкурентоспроможними.

Особливе значення мають ризики, пов'язані з появою нових гравців на ринку. Нові компанії можуть пропонувати інноваційні продукти, агресивні маркетингові стратегії або нижчі ціни, що підриває позиції існуючих гравців. Такі конкуренти часто швидко адаптуються до ринкових умов і можуть привертати увагу цільової аудиторії, особливо молодших і більш технологічно підкованих користувачів. Поява нових гравців змушує компанії постійно оновлювати свою пропозицію, покращувати якість обслуговування,

впроваджувати нові технології і знаходити способи збереження лояльності клієнтів.

Щоб зменшити вплив нових конкурентів, компанії застосовують різні стратегії: інноваційний розвиток продуктів та послуг, створення унікальних пропозицій, побудову сильного бренду та активну комунікацію з аудиторією. Важливим є також аналіз конкурентного середовища, прогнозування появи нових гравців та планування сценаріїв реагування на зміни ринку. Постійна увага до конкурентів дозволяє зберегти стійкість бізнесу, підтримувати конкурентні переваги та мінімізувати ризики втрати частки ринку.

Ще одним важливим конкурентним ризиком є ціновий тиск. У світі електронної комерції споживачі легко порівнюють ціни між різними платформами, і будь-яке невелике підвищення може швидко відлякати клієнтів. Конкуренти часто використовують агресивні акції, знижки або безкоштовну доставку, щоб залучити аудиторію, що змушує компанії постійно шукати баланс між прибутковістю та привабливими пропозиціями для клієнтів.

Також існує ризик втрати клієнтів через інновації конкурентів. Якщо інший гравець на ринку запускає новий функціонал, більш зручний сервіс або унікальні продукти, частина клієнтів може мігрувати до нього. Наприклад, поява сервісів із миттєвою доставкою або інтерактивними онлайн-консультаціями створює очікування, що компанія повинна швидко адаптуватися, щоб не відстати від ринку.

Ризики технологічного відставання теж дуже помітні в електронному бізнесі. Технології розвиваються надзвичайно швидко: поки одна компанія працює на старій платформі, конкуренти можуть впроваджувати автоматизацію, штучний інтелект або персоналізовані рекомендації, що підвищує їхню привабливість для споживачів. Відставання в технологіях одразу впливає на конкурентоспроможність і може призвести до втрати ринку.

Не менш значущим є ризик втрати репутаційної переваги. Якщо конкурент завоював довіру аудиторії через прозорість, якість обслуговування або соціальні ініціативи, компанії, що не розвивають ці напрямки, можуть опинитися в тіні. Споживачі часто обирають не найдешевший товар, а той, у якого бренд асоціюється з надійністю і відповідальністю.

Нарешті, ризик надмірної концентрації на окремих каналах збуту теж є конкурентним. Якщо бізнес сильно залежить від однієї платформи чи технології, конкуренти, які освоюють нові канали продажу або соціальні мережі, можуть швидко відбирати аудиторію. Наприклад, магазини, що працюють лише через сайт, ризикують втратити клієнтів до мобільних додатків або маркетплейсів із інтегрованими платіжними системами.

Щоб уникнути негативного впливу появи нових гравців на ринку, компанії повинні постійно стежити за конкурентним середовищем і прогнозувати потенційні загрози. Важливо впроваджувати інновації, створювати унікальні продукти або сервіси, які складно повторити новачкам, а також активно розвивати бренд і підвищувати лояльність клієнтів через персоналізовані пропозиції та якісне обслуговування.

Подолання цінового тиску передбачає гнучку політику ціноутворення і стратегічне планування акцій. Компанії можуть застосовувати диференціацію пропозицій, додавати додаткові сервіси, бонуси або програми лояльності, щоб клієнти бачили цінність не тільки у вартості товару, а й у загальному досвіді покупки.

Щоб зменшити ризик втрати клієнтів через інновації конкурентів, потрібно активно впроваджувати технологічні новинки: автоматизацію процесів, персоналізацію контенту, інтерактивні сервіси та покращення мобільного досвіду користувачів. Це дозволяє утримати увагу клієнтів і створити відчуття сучасності та зручності.

Ризик втрати репутаційної переваги можна мінімізувати через прозору комунікацію, підтримку високих стандартів обслуговування, соціальну відповідальність та активну роботу зі спільнотою. Компанії, що вчасно

реагують на критичні ситуації та позитивно взаємодіють із клієнтами, зберігають довіру і підвищують власну конкурентоспроможність.

Нарешті, для зменшення ризику надмірної концентрації на окремих каналах продажу компанії повинні диверсифікувати канали збуту: інтегрувати маркетплейси, соціальні мережі, мобільні додатки та офлайн-партнерства. Такий підхід дозволяє не залежати від одного джерела аудиторії і швидко адаптуватися до змін на ринку.

Комплексний підхід до конкурентних ризиків передбачає одночасну роботу в кількох напрямках: стратегічне планування, інновації, технологічне оновлення, управління репутацією та диверсифікація каналів продажу. Тільки поєднання цих дій дозволяє компанії не тільки уникати загроз, а й використовувати конкурентне середовище як можливість для зростання та розвитку.

Поява електронного бізнесу в середині 1990-х років відкрила новий рівень конкуренції. Amazon, заснований у 1995 році як онлайн-книгарня, показав, як швидкий вихід на ринок і розширення асортименту можуть змінити правила гри. Традиційні книгарні, що діяли локально, опинилися під сильним тиском, адже споживачі отримували доступ до більшого вибору товарів, можливості порівняти ціни та замовити доставку додому. Amazon швидко почав впроваджувати логістичні інновації, оптимізуючи склади та доставку, що забезпечило йому стійку конкурентну перевагу.

Одночасно на ринку з'являлися інші нові компанії, такі як eBay, який відкрив онлайн-аукціони для приватних продавців. Це спричинило ризики для традиційних аукціонів і локальних оголошень, адже покупці почали переміщатися в інтернет-простір. Компанії були змушені адаптуватися, створюючи власні платформи або інтегруючи нові моделі продажу.

У кінці 1990-х років пошукові системи, особливо Google, значно вплинули на конкурентне середовище. Компанії, які не використовували інструменти оптимізації пошукових запитів, втрачали значну частку трафіку та потенційних клієнтів. Це стало прикладом того, як технологічні зміни

формують нові конкурентні ризики, змушуючи бізнес швидко реагувати і впроваджувати інновації.

На початку 2000-х років багато нових інтернет-компаній зазнали краху внаслідок дотком-кризи. Високий приплив стартапів із нестабільними бізнес-моделями показав, що конкуренція може бути надзвичайно жорсткою, а виживають лише ті компанії, які поєднують фінансову стійкість, стратегічне планування та здатність до адаптації. Одночасно це створило уроки для ринку щодо управління ризиками та важливості диференціації продуктів.

У середині 2000-х років з'явилися глобальні маркетплейси, такі як AliExpress, Amazon Marketplace та Rakuten, що збільшило доступність товарів для споживачів і значно підвищило конкуренцію для локальних магазинів. Тепер компанії мали не лише відповідати ціновим очікуванням клієнтів, а й постійно впроваджувати інновації, покращувати сервіс, швидко реагувати на зміни попиту та пропонувати програми лояльності. Поява нових гравців змусила компанії шукати шляхи диверсифікації каналів продажу та зміцнювати власний бренд, щоб зберегти конкурентні позиції.

Питання для обговорення:

1. Які способи моніторингу конкурентного середовища є найефективнішими для електронного бізнесу?
2. Аналіз прикладів, коли поява нових гравців на ринку змінила стратегію існуючих компаній
3. Як диференціація продукту допомагає уникати цінового тиску конкурентів?
4. Розробка плану впровадження технологічних інновацій для утримання клієнтів
5. Які кроки компанія може зробити, щоб зберегти репутаційні переваги перед конкурентами?
6. Визначення стратегій диверсифікації каналів збуту та їх вплив на стійкість бізнесу

7. Приклади ситуацій, коли відсутність інновацій призвела до втрати частки ринку

8. Як програми лояльності та бонусні системи допомагають протидіяти ризикам втрати клієнтів?

9. Оцінка впливу агресивних маркетингових стратегій конкурентів на поведінку споживачів

Тема 11. Ризики інтелектуальної власності.

Мета: ознайомити студентів із сутністю ризиків, пов'язаних з інтелектуальною власністю в електронному бізнесі, їхніми джерелами та наслідками для компаній, а також розглянути стратегії захисту авторських прав, патентів, торгових марок і комерційних секретів.

Ризики інтелектуальної власності виникають у цифровому бізнесі через високий рівень доступності інформації, легкість копіювання продуктів і послуг, а також глобальний характер онлайн-платформ. Основними загрозами є незаконне використання авторських прав, порушення патентів, неправомірне використання торгових марок та витік комерційної інформації. Такі ризики можуть призвести до фінансових втрат, втрати конкурентної переваги, пошкодження репутації та юридичних конфліктів із іншими компаніями.

Особливу увагу слід приділити порушенню авторських прав. У електронному бізнесі це проявляється у копіюванні дизайну сайту, контенту, програмного забезпечення або мультимедійних матеріалів без дозволу власника. Порушення авторських прав може призвести до судових позовів, штрафів та втрати довіри клієнтів, особливо якщо клієнти виявляють недобросовісність компанії.

Ще одним ризиком є порушення патентів та комерційних секретів. Конкуренти можуть копіювати запатентовані технології, алгоритми або бізнес-процеси, що зменшує унікальність продукту і підриває стратегічні переваги. Витоки комерційної інформації, таких як внутрішні дані про

розробки, маркетингові стратегії або клієнтські бази, створюють додаткові загрози для бізнесу та можуть стати основою для судових спорів.

Порушення торгових марок та брендингу також становить серйозний ризик. Незаконне використання імені компанії або логотипу іншими суб'єктами може ввести споживачів в оману, знизити довіру до бренду і вплинути на лояльність клієнтів. У цифровому середовищі це особливо критично через швидке поширення інформації і глобальний доступ до онлайн-магазинів і платформ.

Ефективне управління ризиками інтелектуальної власності включає комплекс заходів: реєстрацію авторських прав, патентів і торгових марок, використання ліцензійних угод, контроль за витоком комерційної інформації, моніторинг конкурентів і інтернет-простору, а також оперативне реагування на порушення прав. Компанії, що активно захищають свою інтелектуальну власність, зберігають унікальність продуктів, підвищують довіру споживачів і мінімізують фінансові та репутаційні ризики.

Захист авторських прав передбачає реєстрацію оригінального контенту, програмного забезпечення, мультимедійних матеріалів і дизайну сайтів. Компанії активно використовують ліцензійні угоди, щоб офіційно дозволяти використання своїх матеріалів сторонніми особами, а також впроваджують технології цифрового водяного знаку і DRM (Digital Rights Management), що ускладнює незаконне копіювання та поширення контенту.

Щодо патентів, компанії реєструють винаходи, алгоритми, технічні рішення та унікальні бізнес-процеси, щоб забезпечити правовий захист і виключити несанкціоноване використання конкурентами. Крім того, важливо проводити моніторинг ринку на предмет можливих порушень і швидко реагувати на спроби копіювання або незаконного використання запатентованих рішень.

Захист торгових марок і бренду полягає у реєстрації логотипів, назв, слоганів та унікальної айдентики компанії. Це дозволяє попереджати плутанину серед споживачів і запобігати недобросовісній конкуренції.

Важливим також є регулярний моніторинг онлайн-платформ і соціальних мереж, щоб виявляти спроби несанкціонованого використання бренду та оперативно реагувати на порушення.

Для збереження комерційних секретів компанії застосовують внутрішні політики безпеки, обмеження доступу до конфіденційної інформації, шифрування даних, підписання угод про нерозголошення (NDA) з працівниками і партнерами, а також аудит і контроль внутрішніх процесів. Це дозволяє мінімізувати ризики витоку стратегічних даних, клієнтських баз, маркетингових планів або розробок продуктів.

Комплексне впровадження цих стратегій забезпечує компанії захист інтелектуальної власності, підтримку конкурентної переваги та збереження довіри клієнтів. Активна робота у всіх напрямках дозволяє перетворити інтелектуальну власність на стабільний актив, який генерує додаткову цінність для бізнесу та запобігає юридичним і фінансовим проблемам.

Наслідки ризиків інтелектуальної власності в електронному бізнесі можуть бути досить серйозними та багатовимірними:

1. **Фінансові втрати.** Незаконне використання авторських прав, патентів або торгових марок може призвести до прямих витрат на судові позови, штрафи, компенсації або відшкодування збитків. Крім того, втрата унікальних рішень та технологій зменшує прибуток і знижує рентабельність бізнесу.

2. **Втрати конкурентної переваги.** Якщо конкуренти копіюють запатентовані технології, бізнес-процеси або унікальні рішення, компанія втрачає унікальність продукту. Це призводить до зниження лояльності клієнтів, відтоку аудиторії та підвищення цінової конкуренції.

3. **Пошкодження репутації.** Витік комерційної інформації або незаконне використання бренду може негативно вплинути на імідж компанії. Споживачі можуть втратити довіру, якщо бачать недобросовісну поведінку або підроблені товари під брендом компанії.

4. Юридичні конфлікти. Порушення прав інтелектуальної власності часто призводить до тривалих судових процесів із високими витратами на адвокатів і судові збори. Водночас програні справи можуть обмежувати можливості компанії на певних ринках або забороняти використання ключових продуктів.

5. Втрата стратегічних даних. Витоки комерційної інформації, таких як клієнтські бази, маркетингові плани або внутрішні розробки, можуть дозволити конкурентам швидко адаптуватися до бізнес-моделі компанії і посилити їхню позицію на ринку.

6. Обмеження розвитку та інновацій. Якщо компанія боїться втратити патенти або авторські права, це може стримувати її від відкритого обміну ідей або впровадження нових технологій. Недостатній захист інтелектуальної власності демотивує інвесторів і партнерів.

У підсумку, ризики інтелектуальної власності без належного управління можуть призвести до значних фінансових, репутаційних і стратегічних втрат. Водночас ефективний захист — через реєстрацію прав, ліцензійні угоди, внутрішні політики безпеки та моніторинг ринку — дозволяє перетворити інтелектуальну власність на стабільний актив і джерело конкурентної переваги.

Питання для обговорення:

1. Які заходи найефективніше захищають авторські права в цифровому середовищі?
2. Аналіз прикладів, коли відсутність патентного захисту призвела до втрати конкурентної переваги
3. Розробка стратегії моніторингу використання торгових марок компанії в інтернеті
4. Як ліцензійні угоди допомагають контролювати використання інтелектуальної власності?
5. Приклади витоку комерційних секретів і наслідки для бізнесу

6. Які технології цифрового захисту (DRM, водяні знаки) найбільш ефективні для контенту?

7. Розробка внутрішніх політик та процедур для запобігання несанкціонованому доступу до даних

8. Визначення стратегій швидкого реагування на порушення інтелектуальних прав конкурентами

Тема 12. Управління ризиками в міжнародному електронному бізнесі.

Мета: ознайомити студентів із специфікою управління ризиками в міжнародному електронному бізнесі, показати джерела цих ризиків та методи їх ідентифікації, аналізу й мінімізації для забезпечення ефективної діяльності компанії на глобальних ринках.

Міжнародний електронний бізнес стикається з унікальними ризиками через глобальну природу ринку, різноманітність правових систем, валютні коливання, культурні та мовні відмінності, а також різні стандарти безпеки та конфіденційності. Ці ризики можуть впливати на фінансові результати, репутацію компанії та довіру клієнтів у різних країнах.

Однією з ключових складових управління ризиками є політика комплаєнсу та дотримання місцевого законодавства. Компанії повинні враховувати різні регуляторні вимоги щодо електронної комерції, оподаткування, захисту даних та інтелектуальної власності. Недотримання правил може призвести до штрафів, блокування діяльності на окремих ринках і втрати клієнтів.

Ще одним важливим аспектом є фінансовий ризик міжнародних операцій, що включає валютні коливання, різні платіжні системи та можливі проблеми з трансфером коштів. Для мінімізації цих ризиків компанії застосовують хеджування, використання надійних платіжних платформ та моніторинг фінансових потоків у різних країнах.

Культурні та соціальні відмінності також створюють ризики для бізнесу. Неправильне розуміння локальних уподобань, традицій або законів

про рекламу та маркетинг може призвести до негативної реакції споживачів, репутаційних втрат і падіння продажів. Ефективна локалізація продуктів, сервісів і комунікацій дозволяє уникати цих ризиків і підвищує конкурентоспроможність.

Технологічні та інформаційні ризики у міжнародному бізнесі пов'язані з безпекою даних, адаптацією ІТ-систем до різних стандартів та забезпеченням безперебійної роботи платформ у різних країнах. Компанії застосовують шифрування, багатофакторну автентифікацію, резервне копіювання та регулярні аудити безпеки для зниження цих ризиків.

Управління міжнародними ризиками передбачає комплексний підхід: моніторинг глобального ринку, аналіз правових, фінансових та технологічних факторів, локалізацію продуктів і сервісів, навчання персоналу та розробку стратегій швидкого реагування на інциденти. Такий системний підхід дозволяє компанії ефективно працювати на глобальному рівні, мінімізувати загрози і використовувати міжнародний ринок як можливість для зростання та розвитку.

1. Методи ідентифікації ризиків

Ідентифікація ризиків передбачає виявлення всіх потенційних загроз ще до того, як вони почнуть впливати на діяльність компанії. Моніторинг зовнішнього середовища дозволяє відстежувати зміни у законодавстві, політичну нестабільність, економічні тенденції та конкурентну активність на різних ринках. Аналіз регуляторних вимог і комплаєнсу допомагає визначити країни та регіони, де існують особливі обмеження для електронної комерції, наприклад, щодо захисту персональних даних чи оподаткування. Аудит технологічної інфраструктури дозволяє виявити слабкі місця в ІТ-системах, що можуть призвести до витоків даних або збоїв у роботі платформи. Опитування локальних команд та споживачів допомагає ідентифікувати культурні, соціальні та мовні бар'єри, які можуть впливати на сприйняття продукту. Аналіз діяльності конкурентів і фінансових тенденцій дозволяє

передбачити загрози від агресивних стратегій конкурентів або зміни попиту на ринку.

2. Методи аналізу ризиків

Після виявлення ризиків їх необхідно оцінити за критеріями ймовірності та впливу на бізнес. SWOT-аналіз на міжнародному рівні дозволяє систематизувати сильні та слабкі сторони компанії, а також можливості та загрози на кожному ринку. Сценарний аналіз фінансових ризиків допомагає передбачити наслідки валютних коливань, зміни тарифів на міжнародні платежі та вплив економічних криз. Ризикове картування технологічних і інформаційних загроз дозволяє визначити, які системи є критично важливими, де можливі збої та як вони вплинуть на операційну діяльність. Аналіз потенційного репутаційного та соціального впливу включає оцінку реакції клієнтів на продукти та комунікації, що допомагає передбачити негативні наслідки помилок або кризових ситуацій.

3. Методи мінімізації ризиків

Мінімізація ризиків спрямована на зменшення ймовірності виникнення загроз і зниження їхнього негативного впливу. Впровадження комплаєнс-програм і локальних політик дотримання законодавства дозволяє уникати штрафів, блокування платформ і юридичних конфліктів у різних країнах. Хеджування фінансових ризиків, використання захищених платіжних систем і резервування валютних потоків допомагає захистити компанію від валютних коливань і проблем з міжнародними платежами. Технологічний захист даних, включно з шифруванням, багатофакторною автентифікацією та резервним копіюванням, знижує ймовірність витоків і збоїв. Локалізація продуктів і маркетингових кампаній враховує мовні, культурні та соціальні особливості ринків, забезпечуючи кращий досвід для клієнтів. Навчання персоналу підвищує готовність команди до кризових ситуацій, а розробка планів реагування дозволяє швидко і ефективно мінімізувати наслідки непередбачених подій.

Найсуттєвіші міжнародні впливи на електронний бізнес пов'язані з глобальною природою ринку та різноманіттям зовнішніх факторів, що можуть прямо чи опосередковано впливати на діяльність компанії. До ключових належать:

1. Правові та регуляторні відмінності. Кожна країна встановлює власні правила електронної комерції, оподаткування, захисту персональних даних та інтелектуальної власності. Несумісність законодавств або недотримання місцевих норм може призвести до штрафів, блокування діяльності, обмеження доступу до ринку та юридичних конфліктів.

2. Фінансові ризики. Валютні коливання, різні платіжні системи та обмеження трансферу коштів впливають на прибутковість і фінансову стабільність компанії. Неправильне управління цими ризиками може призвести до значних збитків та проблем із ліквідністю.

3. Культурні та соціальні відмінності. Мова, традиції, локальні звички споживачів та особливості маркетингових комунікацій впливають на сприйняття продукту. Неврахування цих факторів може викликати негативну реакцію клієнтів, падіння продажів і втрату репутації.

4. Технологічні та інформаційні ризики. В електронному бізнесі важливо забезпечувати безпеку даних, адаптацію ІТ-систем до міжнародних стандартів і безперебійну роботу платформ у різних країнах. Порухення цих умов може призвести до витоків інформації, кібератак або простою сервісу.

5. Конкурентні впливи на міжнародному рівні. Глобальна доступність ринку означає, що конкуренти з інших країн можуть швидко реагувати на тренди, копіювати продукти або пропонувати нижчі ціни, що створює тиск на компанію та зменшує її частку на ринку.

6. Політична та економічна нестабільність. Геополітичні кризи, санкції, зміни митних правил або економічні спади в окремих країнах можуть різко впливати на роботу електронного бізнесу, блокуючи платежі, логістику або доступ до певних ринків.

7. Репутаційні ризики на глобальному рівні. Інформація поширюється миттєво, і негативний відгук у одній країні може вплинути на довіру клієнтів у всьому світі. Втрата репутації на міжнародному ринку може призвести до зниження лояльності та падіння продажів.

В цілому, міжнародний вплив формує складне середовище для електронного бізнесу, де компанії повинні одночасно контролювати правові, фінансові, культурні, технологічні та репутаційні фактори. Ефективне управління ризиками передбачає моніторинг ринку, локалізацію продуктів, комплаєнс-програми, захист даних, фінансове хеджування і гнучкі стратегії реагування на непередбачені події.

Питання для обговорення:

1. Які методи моніторингу зовнішнього середовища є найбільш ефективними для глобального електронного бізнесу?
2. Приклади, коли недотримання локального законодавства призвело до штрафів або блокування діяльності
3. Розробка плану хеджування фінансових ризиків при валютних коливаннях та міжнародних платежах
4. Оцінка ефективності локалізації продуктів і маркетингових кампаній на різних ринках
5. Як внутрішні аудити технологічної інфраструктури допомагають запобігти витокам даних?
6. Аналіз сценаріїв кризових ситуацій і розробка оперативних планів реагування
7. Приклади культурних та соціальних бар'єрів, які вплинули на міжнародні продажі
8. Які інструменти аналітики допомагають прогнозувати появу нових ризиків у глобальному бізнесі?
9. Визначення пріоритетів для управління ризиками: фінансові, технологічні, регуляторні чи репутаційні?

10. Розробка стратегії навчання персоналу для підвищення готовності до міжнародних ризиків

11. Приклади того, як інтеграція ідентифікації, аналізу та мінімізації ризиків забезпечує стабільну діяльність на глобальних ринках

Тема 13. Ризики, пов'язані з шахрайством та недобросовісною конкуренцією.

Мета: ознайомити студентів із сутністю ризиків, пов'язаних із шахрайством та недобросовісною конкуренцією в електронному бізнесі, показати їхні джерела, механізми виникнення та наслідки для компаній, а також розглянути способи запобігання і мінімізації таких ризиків.

Ризики шахрайства та недобросовісної конкуренції в електронному бізнесі виникають через високий рівень доступності цифрових платформ, анонімність користувачів та глобальний характер ринку. Основні прояви цих ризиків включають фінансові шахрайства (незаконне списання коштів, підробка платіжних даних), кібершахрайство (фішинг, хакерські атаки для викрадення інформації), недобросовісну конкуренцію (нелегальне копіювання продуктів, накрутка рейтингів та відгуків, використання чужого бренду або контенту) та маніпуляції з клієнтською довірою.

Шахрайство може призводити до значних фінансових втрат, погіршення репутації компанії, втрати клієнтів та юридичних проблем. Наприклад, підробка платіжних карток або використання фальшивих облікових записів здатна паралізувати роботу електронної платформи і спричинити серйозні витрати на відновлення довіри.

Недобросовісна конкуренція проявляється через навмисне введення в оману споживачів, підрив цінової політики, копіювання інноваційних рішень або використання маркетингових хитрощів для переваги над легальними конкурентами. Це може суттєво зменшити частку ринку компанії та вплинути на її стратегію розвитку.

Для зниження таких ризиків компанії використовують комплексні заходи: впровадження технологій безпеки і моніторингу транзакцій, аудит платіжних систем, контроль за активністю конкурентів у цифровому середовищі, юридичний захист інтелектуальної власності, створення систем повідомлень про підозрілі дії користувачів, навчання персоналу та впровадження внутрішніх політик етичної поведінки.

Системне управління ризиками шахрайства та недобросовісної конкуренції дозволяє зберегти фінансову стабільність, підтримати репутацію бренду, забезпечити довіру клієнтів і створити конкурентні переваги на ринку електронної комерції.

Першим кроком у запобіганні ризикам є технологічний захист. Використання сучасних систем безпеки, таких як багатофакторна автентифікація, шифрування даних, постійний моніторинг транзакцій і активності користувачів, дозволяє знизити ймовірність фінансових шахрайств та кібератак. Системи аналітики та алгоритми виявлення аномалій здатні автоматично ідентифікувати підозрілу поведінку, наприклад, підроблені платежі або масові спроби доступу до акаунтів.

Другим напрямом є юридичний захист і контроль за дотриманням правил. Реєстрація торгових марок, авторських прав та патентів дозволяє запобігати недобросовісному використанню продуктів і контенту конкурентами. Важливо також мати внутрішні політики етичної поведінки і чіткі договори з партнерами, що передбачають штрафи або юридичні санкції у разі порушень.

Третім аспектом є моніторинг конкурентного середовища. Регулярне відстеження дій конкурентів у цифровому середовищі, включно з аналізом цінової політики, маркетингових кампаній, рейтингу та відгуків, дозволяє швидко реагувати на спроби недобросовісної конкуренції та зберігати конкурентні переваги.

Четвертий напрям — навчання персоналу та підвищення обізнаності клієнтів. Співробітники повинні знати основні механізми шахрайства та

алгоритми захисту, а клієнти — бути обізнаними про потенційні ризики, наприклад, про фішингові листи або підозрілі сайти. Це дозволяє знизити ймовірність помилок, які можуть призвести до фінансових втрат або репутаційних проблем.

П'ятий напрям — проактивні внутрішні процедури та плани реагування на інциденти. Компанія повинна мати чітко визначені дії у разі виявлення шахрайства чи недобросовісної конкуренції: блокування підозрілих акаунтів, повідомлення правоохоронних органів, оперативне повідомлення клієнтів і відновлення пошкоджених систем. Такий підхід дозволяє мінімізувати негативний вплив на фінанси, репутацію та довіру клієнтів.

Комплексне застосування цих заходів забезпечує високий рівень захисту електронного бізнесу від шахрайства і недобросовісної конкуренції, дозволяє підтримувати стабільну роботу платформи, зберігати клієнтську базу та забезпечує довгострокову конкурентну перевагу.

Ось кілька найгучніших випадків шахрайства та недобросовісної конкуренції в електронному бізнесі, які ілюструють, до чого можуть призвести такі ризики:

1. Target і витік даних (2013)

Масштабна хакерська атака на американську мережу Target призвела до крадіжки інформації понад 40 млн платіжних карток клієнтів. Компанія зазнала фінансових втрат понад 200 млн доларів на покриття компенсацій та судові витрати, а також значно постраждала репутація бренду. Цей кейс показав, як кібератаки можуть паралізувати роботу компанії та знизити довіру клієнтів.

2. Sony PlayStation Network (2011)

Кіберзлочинці зламали сервери Sony, викравши дані близько 77 млн користувачів. Через інцидент PlayStation Network була недоступна більше трьох тижнів, що спричинило значні фінансові втрати та падіння довіри

користувачів. Цей випадок підкреслив важливість технологічного захисту та швидкого реагування на інциденти.

3. Amazon і накрутка відгуків

У 2015–2019 роках виявлено численні випадки, коли продавці на Amazon використовували фейкові акаунти для підвищення рейтингу продуктів. Це створювало недобросовісну конкуренцію та вводило споживачів в оману. Amazon впровадила алгоритми виявлення підроблених відгуків і санкції для недобросовісних продавців, але кейс показав, наскільки легко цифрові платформи можуть стати об'єктом маніпуляцій.

4. eBay і підробка лотів

У середині 2010-х на eBay активно продавалися підробки відомих брендів. Споживачі купували «оригінали», але отримували фальшиві товари. Це призвело до численних судових процесів і втрати довіри клієнтів до платформи, змусивши eBay запровадити більш жорсткий контроль за продавцями та інтегрувати програми захисту покупців.

5. Facebook і фейкові акаунти з політичною рекламою (2016–2018)

Маніпуляції через створення фейкових акаунтів і недобросовісну рекламу вплинули на політичні кампанії та знизили довіру користувачів до платформи. Facebook змушений був вжити заходів із перевірки рекламодавців і підвищення прозорості, показавши, що шахрайство може впливати не лише на фінанси, але і на репутацію та соціальний контекст.

6. Alibaba і фальшиві товари

На китайській платформі Alibaba протягом років продавалися контрафактні товари під відомими брендами. Це створювало недобросовісну конкуренцію, шкодило репутації брендів і загрожувало міжнародним партнерствам. Alibaba активно впровадила системи перевірки продавців та механізми боротьби з підробками, однак випадок показав масштабність проблеми у глобальному електронному бізнесі.

Ці кейси демонструють, що наслідки шахрайства та недобросовісної конкуренції включають фінансові збитки, втрату довіри клієнтів, юридичні

суперечки, падіння репутації бренду та необхідність серйозних технологічних та управлінських заходів для відновлення позицій на ринку.

Питання для обговорення:

1. Які технології виявлення фішингових атак найбільш ефективні для онлайн-магазинів?
2. Аналіз кейсів, коли недобросовісне використання чужого бренду призвело до падіння продажів
3. Методи контролю та верифікації онлайн-відгуків для запобігання накруткам
4. Як системи моніторингу транзакцій допомагають запобігати фінансовим шахрайствам?
5. Розробка внутрішніх протоколів реагування на спроби кібершахрайства
6. Приклади використання правового захисту для боротьби з копіюванням продуктів конкурентами
7. Стратегії навчання персоналу виявляти ознаки шахрайства та підозрілі дії користувачів
8. Аналіз впливу підроблених акаунтів на репутацію електронного бізнесу
9. Використання алгоритмів машинного навчання для автоматичного виявлення аномалій у поведінці клієнтів
10. Методи інтеграції технологічного, юридичного та організаційного захисту для мінімізації ризиків шахрайства

Тема 14. Ризики масштабування та зростання електронного бізнесу.

Мета: ознайомити студентів із сутністю ризиків, які виникають під час масштабування та зростання електронного бізнесу, показати їхні джерела, можливі наслідки та способи управління для забезпечення стабільного розвитку компанії на різних ринках.

Масштабування електронного бізнесу передбачає збільшення обсягів продажів, розширення клієнтської бази, вихід на нові ринки та інтеграцію додаткових сервісів. Проте цей процес супроводжується значними ризиками, які можуть загрожувати стабільності компанії. Основні категорії ризиків включають фінансові, операційні, технологічні, організаційні та репутаційні.

Фінансові ризики виникають через великі інвестиції у розширення інфраструктури, маркетингові кампанії та логістичні операції. Неконтрольоване зростання витрат може призвести до фінансової нестабільності та зниження рентабельності. Операційні ризики пов'язані з перевантаженням внутрішніх процесів, затримками у виконанні замовлень, помилками в управлінні запасами та логістикою.

Технологічні ризики включають несправності систем, недостатню масштабованість платформ, проблеми з обробкою великих обсягів даних та збої в роботі онлайн-сервісів. Недостатня готовність IT-інфраструктури до зростання навантаження може призвести до зниження продуктивності, втрати клієнтів та репутаційних втрат.

Організаційні ризики виникають через необхідність збільшення штату, навчання нових співробітників, зміни у внутрішній структурі та управлінні командами. Недостатня координація та слабка комунікація можуть створити хаос у процесах і сповільнити розвиток бізнесу.

Репутаційні ризики пов'язані з тим, що зростання часто привертає увагу конкурентів та медіа. Будь-які помилки у роботі сервісу або конфлікти з клієнтами можуть мати масштабний ефект і негативно вплинути на імідж компанії.

Для мінімізації цих ризиків компанії використовують комплексний підхід: планування масштабування з урахуванням ресурсів і можливостей, впровадження автоматизованих систем управління процесами, підвищення надійності IT-інфраструктури, ефективне навчання та адаптацію персоналу, а також моніторинг репутації і активна комунікація з клієнтами.

Прогнозування ризиків і готовність до оперативного реагування дозволяють забезпечити стабільний ріст та успішну експансію на нові ринки.

Для уникнення перевантаження інфраструктури компанії впроваджують масштабовані IT-рішення, хмарні сервіси, автоматизовані платформи обробки замовлень та резервні ресурси, що дозволяють підтримувати стабільну роботу навіть при різкому зростанні навантаження.

Щоб подолати нестачу кваліфікованих кадрів, використовують програми навчання та підвищення кваліфікації, залучають віддалених фахівців і створюють системи наставництва, що дозволяє швидко інтегрувати нових співробітників у робочі процеси.

Труднощі з управлінням вирішують через оптимізацію організаційної структури, впровадження прозорих процесів комунікації, регулярні наради та системи контролю за виконанням завдань. Автоматизація управлінських процесів також зменшує ймовірність людських помилок.

Для зниження підвищення витрат застосовують контроль за бюджетом, ефективне планування ресурсів, оптимізацію логістики та закупівель, а також аналіз фінансових потоків для швидкого реагування на відхилення від плану.

Щоб запобігти втратам якості сервісу, впроваджують системи контролю якості, моніторинг клієнтського досвіду, автоматизовану підтримку користувачів, стандартизовані процедури та тестування нових процесів перед масштабуванням.

Питання для обговорення:

1. Які технологічні рішення найефективніше допомагають уникнути перевантаження інфраструктури при різкому зростанні трафіку?
2. Приклади компаній, які зазнали проблем через нестачу кваліфікованих кадрів під час масштабування
3. Стратегії оптимізації організаційної структури для забезпечення ефективного управління під час росту бізнесу
4. Методи контролю бюджету та витрат у процесі масштабування

5. Як автоматизовані системи обробки замовлень можуть запобігти втраті якості сервісу?
6. Методи навчання і адаптації персоналу для підтримки високої продуктивності під час зростання компанії
7. Роль моніторингу клієнтського досвіду у підтриманні репутації під час масштабування
8. Приклади використання хмарних сервісів для забезпечення масштабованості платформи
9. Як прогнозування ризиків допомагає запобігти фінансовим та операційним проблемам при виході на нові ринки

3. ТЕМАТИКА САМОСТІЙНОЇ РОБОТИ

Самостійна робота з теми "Ризики в організації діяльності електронного бізнесу" — це ключова частина навчального процесу, що дає змогу здобувачам вищої освіти самостійно, під керівництвом викладача, поглибити свої знання та розвинути практичні навички.

Виконуючи ці завдання, студенти мають застосувати теоретичний матеріал та набуті прикладні навички для вирішення актуальних проблем у сфері електронного бізнесу. Основна мета — сформулювати вміння проводити науково-дослідну роботу, розвинути творче та критичне мислення, а також навчитися працювати з науковими гіпотезами.

У межах самостійної роботи студентам пропонується обрати та ґрунтовно опрацювати одне з теоретичних питань на вибір, пов'язаних з ризиками в діяльності електронного бізнесу.

4. ПЕРЕЛІК ТЕМ ДЛЯ САМОСТІЙНОЇ РОБОТИ

1. Що таке електронний бізнес і які його ключові особливості?
2. Назвіть основні види ризиків в е-бізнесі.
3. Як класифікуються ризики за джерелами виникнення?
4. Що таке кіберризики та як вони проявляються?

5. Які наслідки можуть мати кібератаки для онлайн-бізнесу?
6. Що таке фінансові ризики в е-комерції?
7. Опишіть операційні ризики електронної платформи.
8. Як впливають технологічні ризики на діяльність онлайн-магазину?
9. Що таке ризики конфіденційності даних клієнтів?
10. Які правові та регуляторні ризики існують в е-бізнесі?
11. Як оцінити репутаційні ризики в соціальних мережах?
12. Що таке ризик шахрайства з платіжними даними?
13. Назвіть методи захисту від фішингу та інших видів шахрайства.
14. Як мінімізувати ризики, пов'язані з логістикою та доставкою?
15. Що таке ризики, пов'язані з залежністю від сторонніх платформ (наприклад, маркетплейсів)?
16. Як впливають конкурентні ризики на стратегію е-бізнесу?
17. Що таке ризики інтелектуальної власності в цифровому середовищі?
18. Як розробити систему управління ризиками в е-бізнесі?
19. Опишіть етапи процесу управління ризиками.
20. Які інструменти використовуються для аналізу ризиків?
21. Що таке матриця ризиків і як її побудувати?
22. Як оцінюється ймовірність і ступінь впливу ризику?
23. Назвіть стратегії реагування на ризики.
24. У чому полягає стратегія уникнення ризику?
25. Що таке страхування ризиків в е-бізнесі?
26. Як впливає людський фактор на виникнення ризиків?
27. Як забезпечити безпеку внутрішніх бізнес-процесів?
28. Які ризики виникають при масштабуванні електронного бізнесу?
29. Що таке бізнес-континуїті (Business Continuity) та як це пов'язано з ризиками?
30. Назвіть приклади ризиків у сфері цифрового маркетингу.
31. Як впливають зміни в законодавстві на ризики е-бізнесу?
32. Що таке ризики, пов'язані з недобросовісною конкуренцією?

33. Як оцінити ефективність заходів з управління ризиками?
34. Яка роль керівництва в управлінні ризиками електронного бізнесу?
35. Як адаптувати стратегію управління ризиками до постійних змін у цифровому середовищі?

5. ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

Політика викладача щодо здобувача освіти

Відвідування занять є обов'язковим компонентом вивчення навчальної дисципліни. Про відсутність з поважних причин здобувачі освіти зобов'язані доводити до відома викладача заздалегідь. За об'єктивних причин (наприклад, хвороба, карантин, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням із деканатом та викладачем.

Політика щодо зарахування результатів формальної, неформальної та інформальної освіти. Результати навчання, здобуті шляхом формальної, неформальної та/або інформальної освіти, визнаються в ВНУ імені Лесі Українки шляхом валідації (https://vnu.edu.ua/sites/default/files/2021-02/Polozhennia_%20vyznannia_rezultativ_navchannia_formalnoi.pdf).

Визнанню можуть підлягати такі результати навчання, отримані в неформальній освіті, які за тематикою, обсягом вивчення та змістом відповідають як освітньому компоненту в цілому, так і його окремому розділу, темі (темам), індивідуальному завданню, контрольній роботі тощо, які передбачені силабусом навчального компонента:

Визнання результатів навчання, отриманих у неформальній та/або інформальній освіті, відбувається в семестрі, що передує семестру початку вивчення освітнього компонента, або першого місяця від початку семестру, враховуючи ймовірність не підтвердження здобувачем результатів такого навчання.

Політика щодо академічної доброчесності.

Жодні форми порушення академічної доброчесності не толеруються. Усі письмові роботи перевіряються на наявність плагіату. Списування під час контрольних робіт та екзамену заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування.

Політика щодо дедлайнів та перескладання.

Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-2 бали). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

6. ПІДСУМКОВИЙ КОНТРОЛЬ

На іспит виносяться основні питання, типові та комплексні задачі, ситуації, завдання, що потребують творчої відповіді та уміння синтезувати отриманні знання і застосовувати їх під час розв'язання практичних задач.

Перелік питань на екзамен

1. Розкрийте сутність поняття "ризик" у контексті електронного бізнесу. Поясніть, чим відрізняються ризики в е-бізнесі від ризиків у традиційній торгівлі.

2. Надайте повну класифікацію ризиків в електронному бізнесі за різними критеріями (джерела, характер, наслідки). Наведіть приклади для кожної групи.

3. Проаналізуйте кіберризики як одну з найважливіших загроз для електронного бізнесу. Опишіть їх види (DDoS-атаки, віруси, фішинг) та механізми захисту.

4. Охарактеризуйте фінансові ризики в е-комерції. Розкрийте поняття ризику транзакцій, ризику несплати, ризику коливання валютних курсів.

5. Поясніть сутність операційних ризиків в електронному бізнесі. Наведіть приклади ризиків, пов'язаних з роботою сайтів, програмного забезпечення та IT-інфраструктури.

6. Розкрийте роль і значення правових та регуляторних ризиків. Проаналізуйте ризики, пов'язані з захистом персональних даних (GDPR), податковим законодавством та авторським правом.

7. Опишіть поняття репутаційних ризиків у цифровому середовищі. Наведіть приклади, як негативні відгуки чи криза в соціальних мережах можуть вплинути на бізнес.

8. Проаналізуйте ризики, пов'язані з конфіденційністю та безпекою клієнтських даних. Які заходи повинні бути вжиті для їх захисту?

9. Охарактеризуйте технологічні ризики. Поясніть, як застаріле програмне забезпечення, проблеми з сумісністю чи збої в роботі технологій можуть вплинути на діяльність компанії.

10. Розкрийте ризики, пов'язані з логістикою та доставкою товарів в е-комерції. Наведіть приклади проблем, що можуть виникнути.

11. Визначте поняття залежності від сторонніх платформ (маркетплейсів, соціальних мереж). Проаналізуйте, які ризики це створює для електронного бізнесу.

12. Проаналізуйте конкурентні ризики в електронному бізнесі. Які стратегії управління цими ризиками існують?

13. Охарактеризуйте ризики інтелектуальної власності. Поясніть, як захистити унікальний контент, торгову марку та інші нематеріальні активи в інтернеті.

14. Розкрийте сутність процесу управління ризиками в електронному бізнесі. Опишіть його основні етапи.

15. Поясніть, як проводиться ідентифікація ризиків. Назвіть інструменти та методи для виявлення потенційних загроз.

16. Проаналізуйте методи кількісної та якісної оцінки ризиків. Наведіть приклади розрахунку ймовірності та впливу ризику.

17. Розкрийте поняття матриці ризиків. Поясніть її структуру та практичне застосування для пріоритезації загроз.

18. Охарактеризуйте стратегії реагування на ризики (уникнення,

передача, зниження, прийняття). Наведіть приклади застосування кожної стратегії.

19. Поясніть, що таке план безперервності бізнесу (Business Continuity Plan) та чому він є важливим для електронного бізнесу.

20. Охарактеризуйте ризики, пов'язані з людським фактором (помилки працівників, несанкціонований доступ, недбалість).

21. Проаналізуйте ризики, що виникають при масштабуванні електронного бізнесу. Поясніть, як зростання може збільшити вразливість.

22. Опишіть ризики, пов'язані з недобросовісною конкуренцією (чорний PR, замовні негативні відгуки, копіювання).

23. Розкрийте поняття етичних ризиків в електронному бізнесі. Наведіть приклади нечесних маркетингових практик чи маніпуляцій з даними.

24. Поясніть роль аудиту безпеки та регулярного моніторингу в управлінні ризиками.

25. Проаналізуйте особливості управління ризиками в міжнародному електронному бізнесі. Які додаткові загрози виникають?

26. Охарактеризуйте ризики, пов'язані з вибором технологічних рішень (CMS, CRM-системи, хмарні сервіси).

27. Розкрийте поняття інвестиційних ризиків в електронному бізнесі. Поясніть, як оцінити потенційну віддачу від інвестицій в стартап чи новий проєкт.

28. Поясніть, як зміни в законодавстві (наприклад, щодо оподаткування) можуть стати джерелом ризиків.

29. Проаналізуйте ризики, пов'язані з кібератаками на платіжні системи. Які механізми захисту існують?

30. Охарактеризуйте ризики, пов'язані з маркетингом та просуванням у цифровому середовищі (ризики рекламних кампаній, SEO-оптимізації).

31. Розкрийте роль корпоративної культури в управлінні ризиками. Як можна підвищити обізнаність співробітників про безпеку?

32. Поясніть, як бізнес може використовувати страхування для передачі ризиків. Наведіть приклади страхових продуктів для е-бізнесу.

33. Охарактеризуйте ризики, пов'язані з роботою з підрядниками та аутсорсингом (розробники, маркетологи, логістичні компанії).

34. Проаналізуйте, як бізнес може підготуватися до кризи, пов'язаної з ризиками. Поясніть роль кризового планування.

35. Опишіть ризики, пов'язані з надійністю хостингу та хмарних сервісів. Які критерії вибору провайдера?

36. Розкрийте роль керівництва в управлінні ризиками. Які обов'язки та відповідальність воно несе?

37. Поясніть, як проводиться моніторинг і контроль ризиків. Чому цей етап є безперервним?

38. Охарактеризуйте ризики, пов'язані з використанням штучного інтелекту та машинного навчання в е-бізнесі.

39. Проаналізуйте, як адаптувати стратегію управління ризиками до постійних змін у технологічному та конкурентному середовищі.

40. Наведіть конкретний приклад відомого інциденту з ризиками в електронному бізнесі (наприклад, витік даних великої компанії) та проаналізуйте, як це вплинуло на компанію та її клієнтів.

Таблиця 1

Шкала оцінювання знань здобувачів освіти за освітнім компонентом

Оцінка в балах	Лінгвістична оцінка	Оцінка за шкалою ECTS	
		оцінка	пояснення
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

7. ПЕРЕЛІК ДЖЕРЕЛ РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна література

1. Громовик, В.В. Управління ризиками в електронній комерції. [монографія]. Львів: [Видавництво], 2021. 250 с.
2. Савченко, А.А. Кібербезпека як елемент стратегії управління ризиками в e-commerce. *Економічний вісник*. 2022. № 3. С. 45–52.
3. Коваль, І.М. Правові аспекти захисту персональних даних в онлайн-бізнесі. *Наукові записки Національного університету "Острозька академія". Серія "Економіка"*. 2023. Вип. 12. С. 112–120.
4. Петренко, О.Л. Методи оцінки операційних ризиків електронних торговельних платформ. *Інноваційна економіка*. 2021. № 5. С. 78–84.
5. Мельник, С.С. Репутаційні ризики електронного бізнесу та інструменти їх мінімізації. *Вісник Хмельницького національного університету*. Серія: Економічні науки. 2022. № 6. С. 201–207.
6. Ризики електронного бізнесу. [Електронний ресурс]. URL: <https://example.com/risks-of-e-business> (дата звернення: 10.08.2025).
7. Іванов, В.О. Модель управління фінансовими ризиками в цифровому середовищі. У: *Матеріали Міжнародної науково-практичної конференції «Цифрова економіка: виклики та можливості»*, Київ, 2022. С. 95–99.
8. Закон України «Про електронну комерцію». [Електронний ресурс]. URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text> (дата звернення: 10.08.2025).
9. Григоренко, А.М. Технологічні ризики та їх вплив на стабільність електронного бізнесу. *Економічний аналіз*. 2023. Том 33. № 4. С. 150–161.
10. Електронна комерція та управління ризиками. [навчальний посібник]. За ред. проф. П.В. Сидоренка. Дніпро: [Видавництво], 2022. 350 с.
11. Павлов К.В., Писанко С.В., Романюк Р.В., Павлова О.М. Стратегія та ризики при реформуванні ринку електроенергетики в регіонах України. *Економічний часопис Волинського національного університету*

імені Лесі Українки: журнал. Луцьк. 2021. №1(25). С.16-27.

12. Павлов Костянтин, Павлова Олена, Павлов Костянтин, Ткачук Юліана, Більо Іван, Цифровізація, як основний фактор розвитку бізнесу, Міжнародний науковий журнал «Інтернаука». Економічні науки. № 17 (117), 2 т., 2021. С. 38-43.

13. Павлова, О., Павлов, К., Шульгач, Н., & Плоскіна, А. (2022). Формування бізнес-стратегії підвищення продовольчої безпеки харчової галузі України у воєнний період. Modeling the development of the economic systems, (4), 116–123. <https://doi.org/10.31891/mdes/2022-6-15>

14. Павлов К. В., Павлова О. М., Спас В. В., Данилюк В. В., Романюк Я. Ю. Оцінка ефективності бізнес-проектів: теорія та практика реалізації. Бізнесінформ № 5_2024. С. 161-167. Doi: <https://doi.org/10.32983/2222-4459-2024-5-161-167>

15. Павлов К.В., Освіцінський Б.Р., Сала Д., Омельчук Б.В., Новосад О.В. Макроекономічна стратегія відновлення газорозподільного ринку на прикладі Плану Маршала. Енергозбереження, Енергетика, Енергоаудит. Економіка. №12(190). 2023. С. 73-84. <http://eee.khpi.edu.ua/article/view/302154>

Інформаційні ресурси

1. Бібліотека ім. В.І. Вернадського. URL: <http://www.nbuv.gov.ua/>
2. Бібліотека ім. В.Г. Короленко. URL: <http://korolenko.kharkov.com/>
3. Студентська електронна бібліотека URL: <http://www.lib.ua-ru.net/>
4. Нормативно-правова база України URL: <http://zakon3.rada.gov.ua/>
5. Державний служба статистики URL: <http://www.ukrstat.gov.ua>
6. Інформаційні ресурси у цифровому репозиторії бібліотеки ВНУ імені Лесі Українки. URL: <https://evnuir.vnu.edu.ua>
7. Кабінет Міністрів України. URL: <http://www.kmu.gov.ua/>.
8. Навчальна платформа LMS Moodle: <https://moodle.vnu.edu.ua/course/view.php?id=2094>

Навчально-методичне видання

Павлова Олена Миколаївна
Павлов Костянтин Володимирович
Мохнюк Анна Миколаївна
Шабала Олександр Петрович

Ризики в організації діяльності електронного бізнесу

Методичні рекомендації

Друкується в авторській редакції

Друк – Волинський національний університет ім. Лесі Українки.

43025, м. Луцьк, просп. Волі, 13.

Тираж 50 прим.