Рисунок 1 - Бізнес- модель успішного розвитку «зеленого» підприємництва

Сталий «зелений» транспорт – один із способів пересування до якого відносять: велосипеди, самокати, електромобілі. Створення зарядних станцій для таких автомобілем є однією форм підприємницької діяльності та напрямів для нових ідей стартапу. Саме український стартап Go To-U потрапив до десятки кращих на міжнародному конкурсі ClimateLaunchpad. Основна ідея заключається в тому, щоб об'єднати прогресивно-відповідальні бізнеси, які будуть за екологічність та прогресивність подальшого розвитку[2].

Література.

1. Державна служба статистики України – http://www.ukrstat.gov.ua/
2. Електронний ресурс - https://www.epravda.com.ua/

КІБЕРБЕЗПЕКА - ВПЛИВ НА РОЗВИТОК ЕКОНОМІКИ ПІДПРИЄМТСВА ТА КРАЇНИ

Васильєва В.Ю., здобувач вищої освіти, vvy200230@gmail.com
факультет інформаційні технології
Науковий керівник: Лаптєва Вікторія Василівна,к.е.н.,доцент
Київський національний торговельно-економічний університет

Сучасний етап розвитку суспільства характеризується впровадженням новітніх технологій, що є ознакою високого рівня

економічного розвитку країни. З розвитком технологій, частішають загрози безпеки данних, а саме хакерські атаки, тож з'явилась нова сфера інформаційних технологій. Метою кібератак зазвичай є отримання доступу до конфіденційної інформації, її зміна або знищення, вимагання грошей у користувачів або порушення нормального бізнес-процесу на підприємстві. Сьогодні, в умовах загальної цифровізації, постає питання важливості посилення кіберберзпеки в Україні цілому так і на окремих суб'єктах – підприємствах, адже підвищення розвитку кібербезпеки неминуче веде до прискорення розвитку підприємств і, як наслідок, зростання добробуту держави.

Кібербезпека – це діяльність, спрямована на захист систем, мереж та програм від цифрових атак за допомогою принципів цілісності, доступності та конфедеційності. Підприємства можуть стикнутися з рядом таких проблем, як «фішинг», витік данних, шкідливе програмне забезпечення, «DDoS-атаки» (атаки на відмову в обсуговуванні), «експлойт нульового рівня» та багато інших. Це в свою чергу може призвести до ряду негативних наслідків, а саме: розголошення відомостей, що є таємницею, порушення достовірності фінансової звітності, несанкціонований доступ до бази данних, викривлення публічної інформації, розрив ділових відносин, зниження цін або обсягів реалізації та інше. Все це вплине на економіку підприємства, як мінімум зниження доходу і як максимум може призвести до банкротства [1,с.3].

Тож керівники повинні зайнятися безпекою свого підприємства аби завадити кібератакам і неминучим негативним наслідкам.

Для підприємств три найважливіші інформаційні активи, які слід ретельно захищати це – дані клієнтів та різні договори. Наступний крок- тест оцінки ризиків. Для цього слід найняти спеціаліста з кібезбезпеки, він проведе дії та скаже які вразливості має підприємство і як їх вирішити. Останній та важливий крок це навчання працівників, щоб можна було вчасно запобігти потенційним атакам на ІТ-системи свого підприємства.

Тому актуальним на сьогодні стає розроблення нових моделей кіберзахисту, в яких враховується весь період атаки, максимальний спектр підходів до оцінки загроз та інше. Серед моделей аналізу кібератак накращі це «Діамантова модель» та «QМодель» (табл.1). Вони застосовуються тільки для аналізу кібератак, для їх формалізації з метою надання відповіді на питання хто, навіщо і яким

чином реалізував кібератаку, надають індикатори компрометації кібератак для подальшої кримінальнотехнічної експертизи [2,с.3].

Таблиця 1 - Найбільш ефективні моделі організації кібербезпеки [2,с.3]

Моделі кібербезпеки	Можливості та особливості застосування
Модель ЛоткіВольтерра	Описує динаміку взаємодії сутностей двох видів - «хижаків» і «жертв». Модель представлена у вигляді системи двох звичайних диференціальних рівнянь першого порядку.
Діамантова модель	Використовується взаємозалежні індикатори, що покращують обмін інформацією про кіберзагрози, підвищення контрольованості аналітичного процесу, підтримка характеристики подій у режимі реального часу.
Q Модель	Дозволяє визначити атрибути кібератаки для з'ясування, чи є кіберінцидент кіберзлочином, допомагає вирішувати весь спектр відповідних питань, як технічні, так і ні інформацію гіпотези для проведення розслідування.
Cyber Kill-Chain Ця	Визначає типовий порядок дій зловмисника для досягнення поставлених цілей. Модель виражає, що для досягнення успіху зловмисник повинен пройти усі вісім етапів: розвідка, озброєння, доставка, зараження, інсталяція, отримання управління, виконання дій, знищення слідів.

Тож для розвитку кібербезпеки потрібні зусилля не тільки з боку підприємств, а й держави. У 2016 році була затвержена перша Стратегія кібербезпеки України, в якій зазначено, що розбудовується Національна телекомунікаційна мережа, забезпечується розвиток системи для виявлення вразливостей і реагування на кіберінциденти та кібератаки та найголовніше утворено Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері [3,с.3].

Наступним важливим кроком було прийняття Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Де зазначено:визначення загальних вимог із кіберзахисту об'єктів критичної інфраструктури, встановлення обов'язкових заходів захисту від кібератa [4,с.3].

Найновіший указ був прийнятий 2021 року- указ Президента України про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України". Позиція є такою, що

забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [4, с.3].

Отже, кібератаки здійснили революцію в розумінні безпеки людей. Тож держава і всі підприємства повинні разом докласти зусиль щодо розробки єдиної стратегії щодо захисту данних. Мають проводитись дослідження щодо розробки кіберзахисту, проводитись навчання, сприяння збільшенню місць у ВНЗ на спеціальність кібербезпека.

Література.

1. Туряниця І.І. Кібербезпека як складова захисту впливу економічної інформаційної безпеки на макро-та мікрорівнях.*Управління соціально-економічними трансформаціями господарських процесів*.зб.матеріалів в доп.учасн.ІІ Міжнар.наук.-практ.конф.Мукачево, 2021.С.120-122.

2. Волот І.О. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання. Центральноукраїнський науковий вісник.Економічний науки.Випуск 3.2019.С.238-247.

3. Про рішення Ради національної безпеки і оборони України. "Про Стратегію кібербезпеки України": Указ Президента України №96/2016 від 27 січня 2016 року.

4. "Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури":Постанова Кабінету Міністрів України від 19.06.2019 № 518.

СУЧАСНІ НАПРЯМКИ В РОЗВИТКУ ПРОДАЖІВ НА РЕКЛАМНОМУ РИНКУ УКРАЇНИ

Василика Є.В., здобувач вищої освіти,
louisavas29@gmail.com
Науковий керівник: Приймук О.Р., к.е.н., доцент
Київський національний торговельно-економічний університет

Сучасні технології постійно розвиваються, тому не дивно, що тенденції в засобах масової комунікації та реклами намагаються не відставати. Сьогодні стало неможливо користуватися давно розробленими та перевіреними стратегіями, кожен місяць приносить нові зміни, функції, технології, механізми, напрями рекламної діяльності, тенденції, тим самим, змінюючи шаблони та реальність. Особливо відчутним ці зміни стають у процесі розвитку Інтернет-реклами та електронної комерції.

Із позицій маркетингу діяльність рекламного ринку являє собою