ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, ЯК ІНСТРУМЕНТ УСУНЕННЯ НЕДОЛІКІВ INTERNET OF THINGS

Соколова А. О., студентка
Науковий керівник: Вайданич Т. В., ст. викладач
Національний лісотехнічний університет України, м. Львів

Історія нашої планети пам’ятає, як людство здійснило 3 промислові революції. Початок 2000-х років характеризується новою епохою технологічної думки - стрімким розвитком Індустрії 4.0. Характерними рисами Індустрії 4.0 є повністю автоматизовані виробництва, на яких керівництво всіма процесами здійснюється у режимі реального часу і з урахуванням мінливих зовнішніх умов. Інструментом впровадження такої автоматизації є технологія Internet of Things (IoT, Інтернет речей), завдяки якій усі предмети побуту споживачів підключені до мережі Інтернет.

Можливість автоматично приймати рутинні рішення забезпечується розвиненою системою «комунікації» речей, яка передбачає здатність пристроїв один одного ідентифікувати, характеризувати стан, передавати один одному дані та обробляти їх. Можливість виконання рутинних рішень дозволяє виключити людину із взаємодії пристроїв, тим самим зробивши цю взаємодію більш автономною, надійною, швидкою, системною та контрольованою. Будучи впровадженим у Індустрії 4.0, Інтернет речей має наступні переваги:

1. гнучкість виробництва досягається відмовою від жорстких «конвеєрних» рішень, що в кінцевому рахунку дозволяє масово приймати і виконувати індивідуальні замовлення, простіше впроваджувати у виробництво нові рішення, вільно використовувати аутсорсинг;

2. налаштування виробництва досягається за рахунок його контролю на всіх рівнях і завдяки його функціонуванню на єдиній технологічній платформі;

3. ефективність виробництва пов'язана зі зниженням витрат, пов'язаних з людським фактором: помилок, простоїв, високої вартості людської праці, непрофесійності.

З іншого боку, Інтернет речей може бути впроваджений і в побуті, наприклад, в технологіях розумного будинку, звільняючи людину від рутини.

Система Internet of Things може бути впроваджена майже у всі процеси виробництва, автоматизувавши їх частково або навіть повністю.

За останні декілька місяців одразу три великих компанії, такі як McDonald's, Uber та Johnson & Johnson відмовились від посади директора з маркетингу у своїй структурі [1]. Тепер переважну більшість процесів виконуватиме система автоматизованого маркетингу.

На рисунку 1 графічно представлено процеси, які виконує автоматизований маркетинг.

Рисунок 1 - Схема автоматизації маркетингової діяльності підприємства

Але у той самий час необхідно звернути увагу на суттєві недоліки та серйозні загрози безпеці, які несуть за собою пристрої з підпримкою Інтернету речей. І, як свідчить опитування *Gemalto*, близько 90 % користувачів не довіряють IoT-пристроям. Найбільше респонденти побоюються витоків даних (60 %) і отримання несанкціонованого доступу до особистої інформації (54 %) [2].

Назвати побоювання звичайних користувачів параноєю не можна - експерти теж відзначають, що IoT приносить нові виклики в суспільство, адже одним із головних недоліків безпеки IoT-пристроїв є слабкий вбудований захист.

Тема кібербезпеки вже давно гостро стоїть у всьому світі. За даними дослідження *McAfee* і *CSIS*, світовий збиток від хакерських атак вже досягає $ 600 млрд на рік [3]. «Цифровий світ проник майже в кожен аспект нашого життя. Тепер злочини стали більш прибутковими, менш ризикованими і ніколи не були настільки легкими» - зазначив головний технічний директор *McAfee* Стів Гробман, коментуючи підсумки дослідження.

Щоб розуміти масштаб проблеми варто зазначити, що не так давно стало відомо, що дев'ять країн ЄС налаштовані створити групи швидкого реагування для протидії кібератакам в рамках нового пакту про оборону Євросоюзу. У тому числі за словами співзасновника платформи *Hacken, CEO Information Security Group* Єгора Аушева, новий поштовх для розвитку кібербезпеки дасть «*Загальний регламент про захист персональних даних*»: «тепер усі компанії в світі, в тому числі і в Україні, зобов'язані належним чином зберігати персональні дані громадян і компаній ЄС. Штрафи в разі витоку інформації досягають мільйонів євро» [4].

Згідно рейтингу, складеного на основі Глобального індексу кібербезпеки, у 2018 році Україна зайняла 54 місце з 193, що говорить про доволі низький рівень кібербезпеки [5]. Отже, коли «*Загальний регламент про захист персональних даних*» вступить в силу, ряд українських підприємств не зможуть експортувати свою продукцію в країни Євросоюзу. Це може привести до зниження обсягів експорту, погіршення репутації вітчизняних брендів на зовнішньому ринку та до суттєвих збитків.

Проте, не лише Євросоюз занепокоєний даною проблемою. Кінцевий споживач також вимагає від сучасних підприємств не менш сучасних рішень.

Все більше компаній у світі нарощують свої витрати на кібербезпеку з метою захисту персональних даних, інфраструктури та ноу-хау. У 2017 році витрати на кібербезпеку виросли на 8 % до 93 млрд. дол. у 2018 році. *Gartner* прогнозує, що протягом декількох років очікується, що витрати досягнуть 1 трлн. дол. [6].

Отже, на сьогоднішній день Internet of Things є невід'ємною потребою сучасного світу в умовах Індустрії 4.0. Але у той самий час він несе за собою негативні наслідки та величезні загрози і саме забезпечення кібербезпеки бізнес-процесів є логічним рішенням проблеми.

Література.

1. В McDonald’s, Uber и J&J больше не будет директоров по маркетингу. Почему и что это значит [Електронний ресурс] // Inc.. – 2019. – Режим доступу до ресурсу: https://incrussia.ru/news/mcdonalds-uber-j-j-marketing/.

2. Прихована загроза: інтернет речей [Електронний ресурс] // Телесфера. – 2018. – Режим доступу до ресурсу: http://www.telesphera.net/blog/internet-of-things.html.

3. Kaplan J. Cybersecurity: Linchpin of the digital enterprise [Електронний ресурс] / J. Kaplan, W. Richter, D. Ware // McKinsey & Company. – 2019. – Режим доступу до ресурсу: https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-linchpin-of-the-digital-enterprise?cid=other-eml-alt-mip-mck&hlkid=f825c46afc1d42cc97adc76864ba2e51&hctky=11339831&hdpid=0a717227-f14f-4f49-8d60-ab0a8e8784e9.

4. Дев'ять країн ЄС домовилися створити кіберсили швидкого реагування [Електронний ресурс] // Mind. – 2018. – Режим доступу до ресурсу: https://mind.ua/news/20186080-devyat-krayin-es-domovilisya-stvoriti-kibersili-shvidkogo-reaguvannya.

5. Global Cybersecurity Index (GCI). // ITUPublications. – 2018. – С. 62–68. – Режим доступу до ресурсу: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

6. Швачка А. Состояние кибербезопасности в Украине: независимая внешняя оценка [Електронний ресурс] / А. Швачка // delo.ua. – 2018. – Режим доступу до ресурсу: https://delo.ua/special/sostojanie-kiberbezopasnosti-v-ukraine-nezavisimaja-vneshnjaja-o-346292/.

ОСОБЛИВОСТІ УПРАВЛІННЯ ПІДПРИЄМСТВОМ В СУЧАСНИХ РИНКОВИХ УМОВАХ ГОСПОДАРЮВАННЯ

Бобро І. І., Шишко А. В., студенти
Науковий керівник: Богданович О. А., ст. викладач
Харківський національний університет сільського господарства імені Петра Василенка

Сьогодні для успішного входження вітчизняних підприємств на світовий ринок необхідно використовувати сучасні технології, пов’язані не лише з процессом управління виробництвом, а й з