ปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์
Factors Affecting the Acceptance to Use the AI in Cyber Security Technology

ศุภวัฒน์ เคหาบาล* และจิโรจน์ บุรณศิริ
วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์

Supawat Khehaban* and Jiroj Buranasiri
College of Innovation, Thammasat University

Received: *May 26, 2025*
Revised: *July 23, 2025*
Accepted: *July 24, 2025*

บทคัดย่อ

งานวิจัยนี้ มีวัตถุประสงค์เพื่อ (1) ศึกษาปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และ (2) วิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นงานวิจัยเชิงปริมาณ เก็บรวบรวมข้อมูลจากผู้รับผิดชอบด้านความปลอดภัยทางไซเบอร์ของหน่วยงานบริษัทจดทะเบียนตลาดหลักทรัพย์แห่งประเทศไทย ที่มีการใช้ระบบดิจิทัลและเทคโนโลยีสารสนเทศในการดำเนินธุรกิจ จำนวน 500 ตัวอย่าง ทำการสุ่มตัวอย่างแบบเจาะจง เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเป็นแบบสอบถาม มีค่าความเที่ยงตรงเชิงเนื้อหา (IOC) อยู่ระหว่าง 0.60-1.00 และมีค่าความเชื่อมั่นด้วยสัมประสิทธิ์แอลฟาของครอนบาค (α) เท่ากับ 0.95 สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ค่าแจกแจงความถี่ ร้อยละ ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน และการวิเคราะห์โมเดลสมการโครงสร้าง ผลการศึกษาพบว่า (1) ปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ บริบทขององค์กร ความคาดหวังในการใช้งาน อิทธิพลทางสังคม การรับรู้ถึงความน่าเชื่อถือ และ การรับรู้ถึงประโยชน์ ค่าน้ำหนักองค์ประกอบเท่ากับ 0.393, 0.611, 0.930, 0.244 และ 0.689 ตามลำดับ โดยมีอำนาจพยากรณ์ร้อยละ 80.6 (R^2= .806) (2) ผลการวิเคราะห์องค์ประกอบพบว่า ปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย 9 ปัจจัย 25 กลุ่มองค์ประกอบ ในส่วนของผลการตรวจสอบความสอดคล้องกลมกลืนของข้อมูลเชิงประจักษ์ พบว่า โมเดลการวิจัยมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยมีค่า CMIN/df = 2.410, GFI = 0.936, AGFI = 0.927 และ RMSEA 0.033

คำสำคัญ: การยอมรับเทคโนโลยี การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ปัญญาประดิษฐ์

Abstract

This research aimed to (1) study the factors affecting the acceptance to use the AI in cyber security technology, and (2) identify the component of factors affecting the acceptance to use the AI in cyber security technology. This research was quantitative research by collecting data from 500 personnels responsible in cyber security of the listed companies using digital and information

*ศุภวัฒน์ เคหาบาล (Corresponding Author)
e-mail: supawat.khe@dome.tu.ac.th

technology in their business operations. The sample were selected by using purposive sampling. The questionnaire was used as the research instrument for data collection. The Index of Item-Objective Congruence (IOC) was between 0.60 and 1.00 and the reliability analysis of the overall test indicated Cronbach's Alpha Coefficient (**α**) at 0.95. The statistics for data analysis were frequency distribution, percentage, mean, standard deviation and structural equation model. The study found that (1) factors affecting the acceptance to use the AI in cyber security technology included organizational context, expectation for use, social influence, perceived trust and perceived usefulness. The factor loadings were 0.393, 0.611, 0.930, 0.244, and 0.689, respectively, with the predictive power of 80.6 (R^2= .806) (2) The results of the exploratory factor analysis found that factors affecting the acceptance to use the AI in cyber security technology consisted of nine factors, twenty-five groups of components. The results of model fit found that the research model was consistent with empirical data, with CMIN/df = 2.410, GFI = 0.936, AGFI = 0.927 and RMSEA 0.033.

Keywords: Technology Acceptance, Cybersecurity, Artificial Intelligence

บทนำ

ปัญญาประดิษฐ์ (Artificial Intelligence) เป็นเทคโนโลยีในสาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ (Computer Science) ประกอบด้วยความรู้ทางวิทยาศาสตร์และวิศวกรรมศาสตร์ การใช้โปรแกรมคอมพิวเตอร์ให้เรียนรู้และเข้าใจความสามารถของมนุษย์และมีความสามารถคล้ายกับมนุษย์โดยใช้ซอฟต์แวร์และฮาร์ดแวร์ เพื่อสามารถทำงานได้แทนมนุษย์หรือเพื่อส่งเสริมกิจกรรมต่าง ๆ ของมนุษย์ให้ดียิ่งขึ้น (ปาริฉัตร วิชุภากรณ์กุล, 2563) ซึ่งความก้าวหน้าและพัฒนาการของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence) ทำให้ในหลาย ๆ ธุรกิจหลีกเลี่ยงไม่ได้ที่จะนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ สำนักงานพัฒนารัฐบาลดิจิทัลคาดการณ์ว่าในอีก 10 ปีข้างหน้า จะถูกนำไปใช้ตั้งแต่ระบบที่ทำงานแบบซ้ำ ๆ ไปจนถึงระบบที่สามารถช่วยทำนาย ช่วยให้ข้อเสนอแนะและช่วยคาดการณ์ในสถานการณ์แบบต่าง ๆ (กระทรวงอุดมศึกษาวิทยาศาสตร์ วิจัย และนวัตกรรม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565)

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึงการปกป้องระบบคอมพิวเตอร์ เครือข่าย และข้อมูลจากการโจมตี การเข้าถึงโดยไม่ได้รับอนุญาต การทำลาย หรือการขโมยข้อมูล โดยใช้เทคโนโลยี กระบวนการ และการควบคุมต่าง ๆ เพื่อป้องกันภัยคุกคามทางไซเบอร์ เช่น แฮกเกอร์ มัลแวร์ และไวรัส เป็นต้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญอย่างยิ่งในยุคดิจิทัล เนื่องจากการโจมตีทางไซเบอร์สามารถก่อให้เกิดความเสียหายทั้งในด้านการเงิน ชื่อเสียง และความเชื่อมั่นขององค์กรและบุคคลทั่วไปได้อย่างมากมาย ดังนั้นการสร้างระบบการรักษาความปลอดภัยนับเป็นสิ่งที่สำคัญเป็นอย่างยิ่งในการนำมาใช้ในองค์กรธุรกิจ เนื่องจากเป็นการป้องกันบุคคลที่เรียกว่า แฮกเกอร์ (Hacker) หรือผู้ที่มีความรู้ความเข้าใจเกี่ยวกับระบบคอมพิวเตอร์ในการหาวิธีการเพื่อเข้าไปขโมยข้อมูลหรือทำลายระบบสร้างความเสียหายให้กับองค์กร ซึ่งการแทรกแซงหรือการโจรกรรมข้อมูลนี้ ถือเป็นปัญหาอาชญากรรมทางด้านเทคโนโลยีที่มีทั่วโลกและมีแนวโน้มเพิ่มมากขึ้นในอนาคต (โกศล จิตวิรัตน์, 2561; อมรรักษ์ สวนชูผล, 2563)

จากผลกระทบได้สร้างความเสียหายให้แก่องค์กรธุรกิจต่าง ๆ เป็นอย่างมาก จึงทำให้เกิดการรักษาความปลอดภัยทางไซเบอร์ขึ้น เป็นแนวปฏิบัติในการปกป้องคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์แอปพลิเคชัน ระบบที่สำคัญและข้อมูล จากภัยคุกคามทางดิจิทัลที่อาจเกิดขึ้นได้ โดยในปัจจุบันมีการใช้ปัญญาประดิษฐ์เพื่อการรักษาความปลอดภัยทางไซเบอร์ โดยระบบปัญญาประดิษฐ์จะสร้างโปรแกรมป้องกันจากการถูกโจมตี ณ ปัจจุบันมีองค์กรระดับโลกที่นำปัญญาประดิษฐ์มาใช้ในการป้องกันภัยไซเบอร์และได้ผลตอบรับที่ดี อาทิเช่น บริษัท Verizon มีระบบ

รักษาความปลอดภัยของอุปกรณ์ภายในเครือข่ายที่ใช้ปัญญาประดิษฐ์ในการบริหารจัดการและประเมินความเสี่ยง เพื่อช่วยให้องค์กรสามารถระบุและจัดลำดับความสำคัญของความเสี่ยงและการบริหารจัดการกับภัยที่มีความรุนแรงได้ดียิ่งขึ้น ฯลฯ จากความสามารถดังกล่าวจะเห็นได้ว่าเทคโนโลยีปัญญาประดิษฐ์มีส่วนช่วยองค์ประธุรกิจในการป้องกันการโจมตีทางไซเบอร์ได้ อีกทั้งยังช่วยลดต้นทุนความเสียหายที่อาจเกิดขึ้นหลังถูกโจมตีทางไซเบอร์ และเพิ่มความน่าเชื่อถือให้กับองค์กรได้อีกด้วย ดังนั้น ผู้วิจัยจึงมีความสนใจที่จะศึกษา ปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยศึกษาในกลุ่มตัวอย่างที่เป็นผู้รับผิดชอบด้านความปลอดภัยทางไซเบอร์ของหน่วยงานบริษัทจดทะเบียนตลาดหลักทรัพย์แห่งประเทศไทย เพื่อนำผลการศึกษามาประยุกต์ใช้ภายในองค์กรให้บุคลากรเกิดการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้มากขึ้น เพื่อประสิทธิภาพที่ดีขึ้นของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

วัตถุประสงค์

1) เพื่อศึกษาปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์

2) เพื่อวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์

แนวคิดทฤษฎีที่เกี่ยวข้องและกรอบแนวคิด

ในการศึกษาปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ผู้วิจัยได้ทำการค้นคว้าและศึกษาทบทวนแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง รวมถึงเอกสารและบทความทางวิชาการ เพื่อให้เกิดความเข้าใจในรายละเอียดเชิงลึกของหัวข้อวิจัยที่ผู้วิจัยต้องการศึกษา ซึ่งมีรายละเอียดในการศึกษา ดังนี้

1. แบบจำลองการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) เป็นแบบจำลองที่มีการพัฒนามาจากพื้นฐานทฤษฎีทางจิตวิทยาสังคม (Social Psychology) โดย Davis (1989) ซึ่งประกอบด้วยทฤษฎีการกระทำด้วยเหตุผล (Theory of Reasoned Action: TRA) และ ทฤษฎีพฤติกรรมที่ได้รับการวางแผน (Theory of Planned Behavior: TPB) โดยแบบจำลองการยอมรับเทคโนโลยี (TAM) ได้รับการยอมรับอย่างกว้างขวางในการทำนายและอธิบายการยอมรับเทคโนโลยี ประกอบด้วยปัจจัย 2 ประการ คือ (1) การรับรู้ประโยชน์จากการใช้เทคโนโลยี (Perceived Usefulness) คือ การรับรู้ความง่ายในการใช้งานถูกอธิบายด้วยความคาดหวังของผู้ใช้งานระบบเทคโนโลยีว่าเป็นระบบที่สะดวกสบายในการเข้าถึง สามารถใช้งานได้ง่าย มีความหลากหลายและครอบคลุมในทุกความต่างของอุปกรณ์ที่เข้าใช้งาน (Hanif and Lallie, 2021) และ (2) การรับรู้ความง่ายต่อการใช้งาน (Perceived Ease of Use) เป็นระดับกระบวนการรับรู้ที่ผู้ใช้งานเชื่อมั่นว่าประโยชน์ของเทคโนโลยี AI จะสามารถปรับปรุงสถานะในการดำเนินงานให้มีประสิทธิภาพและตอบสนองความต้องการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กรได้รวมถึงจะช่วยลดความเสี่ยงในการโจมตีทางไซเบอร์ที่อาจเกิดขึ้น (Yang et al., 2020) ซึ่งจากการทบทวนวรรณกรรมพบว่า การวิจัยของ Hasani et al. (2023) ที่ทำการศึกษา การประเมินการนำความปลอดภัยทางไซเบอร์มาใช้และอิทธิพลที่มีต่อประสิทธิภาพขององค์กร พบว่า ปัจจัยด้านการรับรู้ประโยชน์จากการใช้เทคโนโลยี และ การรับรู้ความง่ายต่อการใช้งาน ส่งผลต่อการนำเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในองค์กรของพนักงาน ซึ่งสอดคล้องกับการศึกษาของ Naw and Kohsuwan (2023) ที่ทำการศึกษาบทบาทของความรู้ ความเสี่ยงที่รับรู้ และความไว้วางใจในการดำเนินการแก้ไขปัญหาความปลอดภัยทางไซเบอร์: การศึกษาในกรุงเทพฯ ประเทศไทย ผลการศึกษาพบว่า การรับรู้ถึงประโยชน์และการรับรู้ความง่ายต่อการใช้งานมีบทบาทสำคัญในองค์กร/ธุรกิจในประเทศไทยและความตั้งใจที่จะนำเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้ ดังนั้นจึงสรุปได้ว่า ปัจจัยการการยอมรับเทคโนโลยี (TAM) มีอิทธิพลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

2. ทฤษฎีการยอมรับและการใช้เทคโนโลยี (The Unified Theory on Acceptance and Use of Technology : UTAUT) ถูกพัฒนาโดย Venkatesh et al. (2003) พัฒนามาจากการศึกษาการรวมกันของทฤษฎีด้านพฤติกรรม 8 ทฤษฎี โดยโครงสร้างของแต่ละทฤษฎีได้ถูกนำมาสนับสนุนและพัฒนาเป็น Model UTAUT โดยโมเดล UTAUT ประกอบไปด้วยปัจจัยหลัก 4 ปัจจัย ได้แก่ (1) ความคาดหวังด้านประสิทธิภาพ (Performance Expectancy) คือ ระดับที่บุคคลเชื่อว่าการใช้ระบบสารสนเทศจะช่วยให้ ความสามารถในการปฏิบัติงานดีขึ้นหรือเชื่อมั่นว่าการใช้ระบบสารสนเทศจะช่วยให้ได้รับประโยชน์ในการทำงาน (Venkatesh et al., 2003) (2) ความคาดหวังในการใช้งาน (Effort Expectancy) คือ ความรู้สึกของแต่ละบุคคลที่รู้สึกว่าไม่ต้องใช้ความพยายามในการใช้เทคโนโลยี (Sair & Danish, 2018) (3) อิทธิพลทางสังคม (Social Influence) คือ ระดับความเข้าใจ ของแต่ละบุคคลที่เชื่อว่าบุคคลรอบข้างมีอิทธิพลต่อตนเองและเชื่อว่าตนเอง ต้องใช้เทคโนโลยีนั้น (Song et al., 2018) และ (4) เงื่อนไขการอำนวยความสะดวก (Facilitating Condition) คือ ระดับที่บุคคลเชื่อว่าโครงสร้างพื้นฐานด้านเทคนิคและโปรแกรมการฝึกอบรมให้ความรู้ที่มีอยู่ภายในองค์กรจะช่วยสนับสนุนการใช้งานระบบเทคโนโลยีใหม่ได้อย่างมีประสิทธิภาพ (Venkatesh et al., 2003) โดยปัจจัยทั้ง 4 ด้านนั้น เป็นปัจจัยที่ส่งผลต่อความเชื่อของผู้ใช้งานเกี่ยวกับ สิ่งอำนวยความสะดวกที่มีอยู่และส่งผลกระทบต่อการยอมรับเทคโนโลยีในบริบทของเทคโนโลยีการทำงานร่วมกัน (Venkatesh, 2016; Rad et al., 2014) ซึ่งสอดคล้องกับการทบทวนวรรณกรรมที่เกี่ยวข้องกับทฤษฎีการยอมรับและการใช้เทคโนโลยีของ Whittaker and Noteboom (2019); Ford (2021); Alneyadi, Kassim and Yin (2022) และ Kumar et al. (2023) ที่พบว่า การยอมรับและการใช้เทคโนโลยีด้านความคาดหวังในการปฏิบัติงาน ความคาดหวังในความพยายาม อิทธิพลทางสังคม และ เงื่อนไขการอำนวยความสะดวก มีอิทธิพลเชิงบวกอย่างมีนัยสำคัญต่อความตั้งใจด้านพฤติกรรมในการยอมรับการใช้งานเทคโนโลยี อีกทั้งยังมีการศึกษาของ Tanantong and Wongras (2023) ที่ได้ทำการศึกษา กรอบการทำงานบนพื้นฐาน UTAUT สำหรับการวิเคราะห์ความตั้งใจของผู้ใช้ในการนำปัญญาประดิษฐ์มาใช้ในการสรรหาบุคลากร: กรณีศึกษาของประเทศไทย ผลการวิจัยพบว่า ปัจจัยด้านความคาดหวังด้านประสิทธิภาพไม่มีอิทธิพลต่อความตั้งใจของผู้ใช้ในการนำปัญญาประดิษฐ์มาใช้ในการสรรหาบุคลากร ดังนั้นจึงสรุปได้ว่า ปัจจัยการยอมรับและการใช้เทคโนโลยี (UTAUT) มีอิทธิพลต่อการยอมรับการใช้ AI และการรับรู้ประโยชน์จากการใช้เทคโนโลยีในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

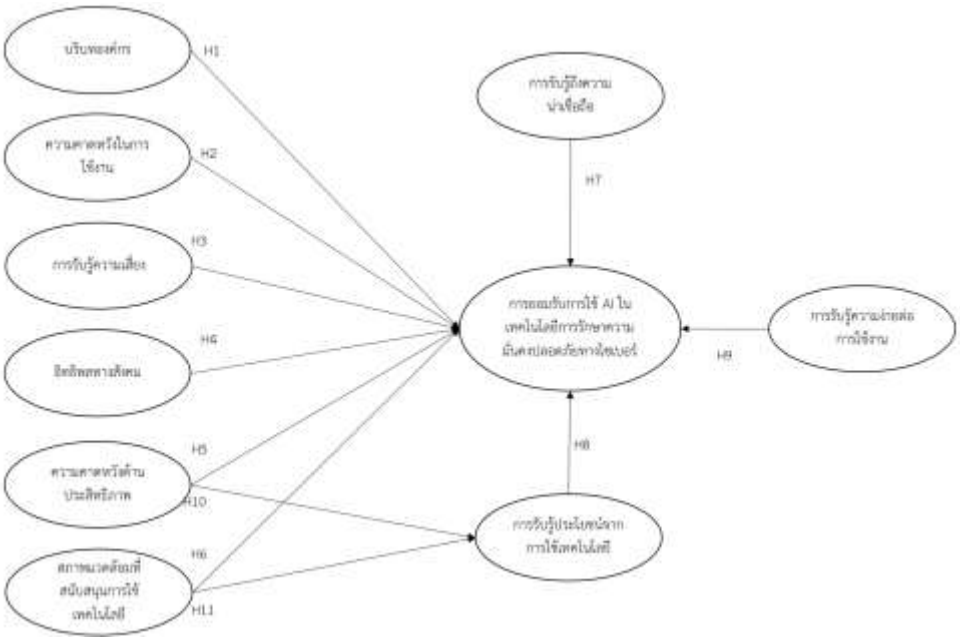
3. แนวคิดเกี่ยวกับบริบทองค์กร (Organizational Context) ตามความหมายใน ISO9000:2015 ได้อธิบายไว้ว่า บริบทองค์กร หมายถึง ปัจจัยหรือสภาพแวดล้อมที่เกิดจากภายในและภายนอกองค์กร และส่งผลกระทบต่อความสามารถขององค์กร เพื่อให้บรรลุตามวัตถุประสงค์และเป้าหมายขององค์กรได้ โดยที่ ณัฐ เลิศฤทธิ์ (2560) กล่าวว่า บริบทองค์กร คือ ข้อมูลพื้นฐานทั่วไป สภาพแวดล้อม ปัจจัยทั้งภายในภายนอกขององค์กร วิสัยทัศน์ พันธกิจ ความสามารถหลักขององค์กร บุคลากร สินทรัพย์ กฎหมาย นโยบายองค์กร ระเบียบข้อบังคับที่เกี่ยวข้องและความสามารถในการแข่งขันที่ผู้บริหารและผู้ที่เกี่ยวข้องจะต้องมีความเข้าใจอย่างแท้จริงเพื่อความสามารถในการแข่งขันขององค์กร ซึ่งจากการทบทวนวรรณกรรมของ Dahabiyeh (2021) ที่ทำการศึกษา ปัจจัยที่ส่งผลต่อการยอมรับขององค์กรและการยอมรับเครื่องมือการฝึกอบรมการรับรู้ด้านความปลอดภัยผ่านคอมพิวเตอร์ ผลการศึกษาพบว่า ปัจจัยด้านองค์กรหรือบริบทต่างๆ ภายในองค์กรนั้น มีอิทธิพลต่อการยอมรับเครื่องมือการรักษาความมั่นคงปลอดภัยผ่านทางคอมพิวเตอร์ ซึ่งเป็นไปในทิศทางเดียวกันกับผลการศึกษาของ ศิริลักษณ์ เมธาธีระนันท์ (2562) ที่พบว่า เกณฑ์การวางนโยบายความปลอดภัยสารสนเทศผู้บริหารด้านสารสนเทศ งบประมาณ และการให้ความสำคัญเรื่องความปลอดภัยด้านสารสนเทศ เป็นปัจจัยที่ส่งผลต่อการยอมรับเทคโนโลยีและการปฏิบัติงานจริงของพนักงานผู้ใช้งานของทุกบริษัท ดังนั้นจึงสรุปได้ว่า ปัจจัยทางด้านบริบทขององค์กรนั้น มีอิทธิพลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

4. แนวคิดเกี่ยวกับการรับรู้ความเสี่ยง (Perceived Risk) คือ การรับรู้ถึงความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้นในการกระทำสิ่งต่าง ๆ ที่ส่งผลให้การกระทำนั้นเกิดความไม่ปลอดภัย ซึ่งความไม่แน่นอนนี้อาจจะมาจาก

หลาย ๆ ปัจจัย เช่น ปัจจัยจากผู้ใช้งาน ปัจจัยจากมิจฉาชีพ ปัจจัยด้านการรักษาความปลอดภัย ปัจจัยทางด้านเทคโนโลยี ซึ่งล้วนนำมาซึ่งความเสี่ยงที่จะเกิดขึ้นในการใช้งานและยังส่งผลในอนาคตอีกด้วย สถานการณ์หรือเหตุการณ์ทั่ว ๆ ไป ที่สามารถพบได้มีความไม่แน่นอน ซึ่งขึ้นอยู่กับโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) ที่จะตามมา (ณัฐพร ไชยยากูลวัฒน์, 2560) จากการทบทวนวรรณกรรมพบว่า มีการศึกษามากมายที่นำปัจจัยการรับรู้ความเสี่ยง (Perceived Risk) มาศึกษาร่วมกับทฤษฎี UTAUT (Abrahão, et al., 2016; Dwivedi, et al., 2017) เนื่องจากมีการศึกษาที่ค้นพบว่า การรับรู้ความเสี่ยงนั้น ส่งผลต่อความตั้งใจใช้งานและการยอมรับเทคโนโลยีของบุคลากรในองค์กรได้ เช่น การศึกษาของ Naw and Kohsuwan (2023) ที่ทำการศึกษาบทบาทของความรู้ ความเสี่ยงที่รับรู้ และความไว้วางใจในการดำเนินการแก้ไขปัญหาความปลอดภัยทางไซเบอร์: การศึกษาในกรุงเทพฯ ประเทศไทย พบว่า การรับรู้ถึงความเสี่ยงของการโจมตีทางไซเบอร์มีบทบาทสำคัญในองค์กร/ธุรกิจในประเทศไทยและความตั้งใจที่จะนำเทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ไปใช้ และการศึกษาของ Kumar et al. (2023) ที่ทำการศึกษา การรับรู้ความเสี่ยงและความน่าเชื่อถือส่งผลต่อการยอมรับบริการธนาคารบนมือถืออย่างไร ผลการศึกษาพบว่า การรับรู้ความเสี่ยง มีอิทธิพลต่อการยอมรับเทคโนโลยีและการใช้งานจริงของผู้ใช้งานเทคโนโลยี ดังนั้นในการศึกษาครั้งนี้ ผู้วิจัยจึงนำปัจจัยการรับรู้ความเสี่ยง (Perceived Risk) มาศึกษาร่วมกับแนวคิดทฤษฎี UTAUT เพื่อให้ทราบถึงปัจจัยด้านการรับรู้ความเสี่ยงที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

5. แนวคิดเกี่ยวกับการรับรู้ถึงความน่าเชื่อถือ (Perceived Trust) กษมา จินุกูล (2562) ได้อธิบายไว้ว่า ความน่าเชื่อถือ คือ ระดับความมั่นใจหรือความไว้ใจในระบบการบริการของผู้ให้บริการว่ามีความน่าเชื่อถือและสามารถให้บริการที่ดีส่งผลให้เกิดประโยชน์แก่ผู้ใช้งานได้ ซึ่งความน่าเชื่อถือของระบบจะถูกเชื่อมโยงเข้ากับการยอมรับเทคโนโลยี หากใช้งานเกิดความไว้วางใจต่อผู้ให้บริการในระดับสูง ก็จะส่งผลให้เกิดการยอมรับเทคโนโลยีและมีความตั้งใจในการใช้งานที่สูงขึ้นตามไปด้วย โดยในการศึกษาของ อคิราภ์ รวมจิตต์ (2564) ระบุว่า การรับรู้ถึงความน่าเชื่อถือ มีความสัมพันธ์ต่อการยอมรับเทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ของผู้ใช้งาน เช่นเดียวกับการศึกษาของ Naw and Kohsuwan (2023) ที่พบว่า ปัจจัยด้านการรับรู้ถึงความน่าเชื่อถือส่งผลต่อทัศนคติที่ดีต่อระบบป้องกันภัยคุกคาม cyber security solutions ซึ่งทัศนคติที่ดีนั้นมีอิทธิพลให้เกิดพฤติกรรมการตั้งใจใช้งานระบบป้องกันภัยคุกคาม cyber security solutions ได้ จากการทบทวนวรรณกรรมข้างต้นจึงสรุปได้ว่า ปัจจัยทางด้านการรับรู้ถึงความน่าเชื่อถือนั้น มีอิทธิพลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

จากการทบทวนวรรณกรรมข้างต้น สามารถสรุปได้ว่า ปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ประกอบไปด้วย 9 ปัจจัย ได้แก่ 1) การรับรู้ประโยชน์จากการใช้เทคโนโลยี (Perceived Usefulness) 2) การรับรู้ความง่ายต่อการใช้งาน (Perceived Ease of Use) 3) ความคาดหวังด้านประสิทธิภาพ (Performance Expectancy) 4) ความคาดหวังในการใช้งาน (Effort Expectancy) 5) อิทธิพลทางสังคม (Social Influence) 6) สภาพแวดล้อมที่สนับสนุนการใช้เทคโนโลยี (Facilitating Condition) 7) บริบทองค์กร (Organizational Context) 8) การรับรู้ความเสี่ยง (Perceived Risk) และ 9) การรับรู้ถึงความน่าเชื่อถือ (Perceived Trust) โดยสามารถกำหนดเป็นกรอบแนวคิดการวิจัยได้ดังแสดงในภาพที่ 1



ภาพที่ 1 ภาพกรอบแนวคิดในการวิจัย

ระเบียบวิธีวิจัย

1. งานวิจัยนี้เป็นการศึกษาวิจัยเชิงปริมาณ (Quantitative Research) โดยมีการกำหนดประชากรและกลุ่มตัวอย่าง คือ พนักงานผู้รับผิดชอบด้านความปลอดภัยทางไซเบอร์ของหน่วยงานของบริษัทจดทะเบียนตลาดหลักทรัพย์แห่งประเทศไทย ที่มีการใช้ระบบดิจิทัลและเทคโนโลยีสารสนเทศในการดำเนินธุรกิจ จำนวน 425 บริษัท กำหนดขนาดของกลุ่มตัวอย่างด้วยวิธี Maximum Likelihoods ของ Lindeman, Merenda and Gold (1980) ระบุไว้ว่าควรกำหนดกลุ่มตัวอย่างควรมีประมาณ 20 มีตัวแปรสังเกตได้จำนวน 24 ตัว กลุ่มตัวอย่างที่เหมาะสมคือ 480 ตัวอย่าง แต่เพื่อให้เกิดความคลาดเคลื่อนน้อยลงจึงกำหนดกลุ่มตัวอย่างเป็นจำนวน 600 ตัวอย่าง และกำหนดวิธีสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) เนื่องจากเป็นการสุ่มตัวอย่างโดยการพิจารณากลุ่มตัวอย่างให้สอดคล้องกับงานวิจัย (อรพรรณ คงมาลัย และ อัญณิฐา ดิษฐานนท์, 2561)

2. เครื่องมือที่ใช้เป็นแบบสอบถามรูปแบบปลายปิด (Close-Ended Questionnaire) ซึ่งเป็นแบบสอบถามที่ได้จากการทบทวนวรรณกรรม แนวคิด ทฤษฎี งานวิจัยต่าง ๆ ที่เกี่ยวข้องกับระดับความคิดเห็นต่อปัจจัยที่ศึกษา โดยมีทางเลือกคำตอบตามมาตรวัดแบบลิเคิร์ท (Likert Scale) 5 ระดับคะแนน

3. ผู้วิจัยได้ทำการพัฒนาแบบสอบถามจากแนวคิด ทฤษฎี การทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง และทำการทดสอบความถูกต้องของเนื้อหา (Content Validity) ด้วยการหาดัชนีความสอดคล้อง (Index of Item Objective Congruence: IOC) ของข้อคำถาม จากการปรึกษากับผู้เชี่ยวชาญจำนวน 5 ท่าน ค่าที่ได้ควรมีค่ามากกว่า 0.50 (สุรพงษ์ คงสัตย์ และ ธีรชาติ ธรรมวงค์, 2558) จึงจะถือว่าข้อคำถามที่ได้พัฒนาขึ้นมามีความเที่ยงตรงของ โดยทดสอบกับกลุ่มทดสอบที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างที่ใช้ในงานวิจัยจำนวน 30 คน และนำมาคำนวณค่าสัมประสิทธิ์ Cronbach’s Alpha องค์ประกอบของแต่ละปัจจัยทุกตัวมีค่าสัมประสิทธิ์ Cronbach’s Alpha อยู่ระหว่าง 0.708 ถึง 0.878 ซึ่งผ่านเกณฑ์ที่กำหนดไว้ที่ควรมากกว่าหรือเท่ากับ 0.70 (Nunnally, 1978)

4. การเก็บรวบรวมข้อมูล ผู้วิจัยแจกแบบสอบถามไปยังกลุ่มตัวอย่าง (Sampling) ผ่านช่องทางออนไลน์รูปแบบ Google Forms จำนวน 425 บริษัท ได้รับแบบสอบถามที่มีความสมบูรณ์กลับมาทั้งสิ้น 500 ชุด

5. วิเคราะห์ข้อมูลด้วยสถิติเชิงอนุมาน (Inferential Statistics) ได้แก่ การวิเคราะห์ปัจจัยเชิงสำรวจ (Exploratory Factor Analysis: EFA) เพื่อตรวจสอบความเที่ยงตรงเชิงโครงสร้างทฤษฎี (Construct Validity) และ

จัดกลุ่มตัวแปรที่มีความเกี่ยวข้องกันให้อยู่ในกลุ่มเดียวกันโดยใช้หลักของความสัมพันธ์เป็นตัวจัดกลุ่ม โดยนำตัวแปรที่มีลักษณะสัมพันธ์กันหรือใกล้เคียงกันจัดไว้ในกลุ่มเดียวกัน (Byrne, 2001) และทำการทดสอบสมมติฐานด้วยการวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) เพื่อตรวจสอบความสัมพันธ์ระหว่างตัวแปร ซึ่งวัดจากความสัมพันธ์ระหว่างตัวแปรแฝง (Latent Variables) และตัวแปรที่สามารถสังเกตได้ (Observed Variables) หรือการวัดความสัมพันธ์ระหว่างตัวแปรตั้งแต่ 2 ตัว ขึ้นไป

ผลการศึกษา

1. การวิเคราะห์ปัจจัยเชิงสำรวจ (exploratory factor analysis: EFA)

ข้อมูลที่ได้จากการเก็บแบบสอบถาม ถูกนำมาวิเคราะห์ปัจจัยเชิงสำรวจเพื่อตรวจสอบความเที่ยงตรงเชิงโครงสร้างทฤษฎี (Construct Validity) และจัดกลุ่มตัวแปรที่มีความเกี่ยวข้องกันให้อยู่ในกลุ่มเดียวกันโดยใช้หลักของความสัมพันธ์เป็นตัวจัดกลุ่ม โดยนำตัวแปรที่มีลักษณะสัมพันธ์กันหรือใกล้เคียงกันจัดไว้ในกลุ่มเดียวกัน และใช้การสกัดองค์ประกอบด้วยวิธี Principal Components หมุนแกนแบบ Varimax เพื่อวิเคราะห์ข้อมูลเป็นไปอย่างมีประสิทธิภาพมากขึ้น โดยกำหนดเกณฑ์การทดสอบ ดังนี้ การทดสอบ Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) ควรมีค่ามากกว่าหรือเท่ากับ 0.50 (Field, 2017) และสถิติทดสอบ Bartlett's Test of Sphericity ควรมีค่า P-value (Sig.) น้อยกว่าระดับนัยสำคัญ 0.05 (Hair et al., 2010) และเกณฑ์การวิเคราะห์องค์ประกอบร่วม ได้แก่ สถิติความแปรปรวนสะสม (Cumulative Percentage of Variance Explained) ควรมีค่ามากกว่าหรือเท่ากับร้อยละ 50.00 ซึ่งจะถือว่าองค์ประกอบใหม่สามารถอธิบายองค์ประกอบโดยรวมได้เพียงพอ ค่าสถิติความร่วมกัน (Communalities) ที่ใช้วัดความสามารถของตัวแปรในการอธิบายองค์ประกอบร่วม ควรมากกว่าหรือเท่ากับ 0.50 และน้ำหนักองค์ประกอบ (Factor Loadings) ใช้แสดงความสัมพันธ์ของตัวแปรกับกลุ่มองค์ประกอบ ควรมากกว่าหรือเท่ากับ 0.50 ซึ่งถือว่ามีนัยสำคัญในทางปฏิบัติและใช้เป็นเกณฑ์ในการจัดกลุ่มองค์ประกอบใหม่ของตัวแปร (Hair et al., 2010) โดยผลการวิเคราะห์องค์ประกอบและการจัดกลุ่มองค์ประกอบใหม่ พบว่า ทุกปัจจัยมีค่า KMO มากกว่า 0.50, ค่า P-value เท่ากับ 0.00, ค่า communalities สูงกว่า 0.5, ค่าสถิติความแปรปรวนสะสมมีค่ามากกว่าร้อยละ 50 และค่าน้ำหนักองค์ประกอบ มีค่ามากกว่า 0.50 โดยผลการสกัดองค์ประกอบพบว่าประกอบไปด้วย 9 ปัจจัยหลัก 25 องค์ประกอบย่อยดังนี้ (รายละเอียดแสดงดังภาพที่ 2)

1.1 ปัจจัยด้านบริบทขององค์กร (Organizational Context) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) การสนับสนุนขององค์กร (Organization Support) 2) การสนับสนุนด้านโปรแกรมและความรู้ (Program and knowledge Support) และ 3) การสนับสนุนจากผู้บริหาร (Leader Support)

1.2 ปัจจัยด้านความคาดหวังในการใช้งาน (Effort Expectancy) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ผลกระทบต่อกันระหว่างปัญญาประดิษฐ์กับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Interacting with AI-driven Cyber security) 2) ความคาดหวังในความง่ายของการใช้งาน (Ease of use) และ 3) เรียนรู้การใช้ประโยชน์จากปัญญาประดิษฐ์ (learning to use AI-powered)

1.3 ปัจจัยด้านการรับรู้ความเสี่ยง (Perceived Risk) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 2 องค์ประกอบ ได้แก่ 1) ผลที่เกิดขึ้นอย่างมิได้ตั้งใจ (Unintended Consequences) และ 2) ความกังวลด้านความเป็นส่วนตัวของข้อมูล (Data Privacy Concerns)

1.4 ปัจจัยด้านอิทธิพลทางสังคม (Social Influence) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ความเชื่อมั่นในระบบปัญญาประดิษฐ์ของผู้นำ (Leaders' confidence in AI) 2) การผลักดันของผู้มีส่วนเกี่ยวข้องในองค์กร (The push in Organizational) และ 3) การริเริ่มนำปัญญาประดิษฐ์มาใช้ในองค์กร (Initiative to use AI in Organizational)

1.5 ปัจจัยด้านความคาดหวังด้านประสิทธิภาพ (Performance Expectancy) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ให้ข้อมูลภัยคุกคามแบบเรียลไทม์ (Provide real-time threat intelligence) 2) ปรับปรุงการตอบสนองต่อเหตุการณ์ (Enhanced incident response) และ 3) ปรับปรุงการตรวจจับภัยคุกคาม (Improved threat detection)

1.6 ปัจจัยด้านเงื่อนไขการอำนวยความสะดวก (Facilitating Conditions) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 2 องค์ประกอบ ได้แก่ 1) ความพร้อมของทรัพยากรที่จำเป็น (Availability of necessary resources) และ 2) โปรแกรมการฝึกอบรม (Presence of training programs)

1.7 ปัจจัยด้านการรับรู้ถึงความน่าเชื่อถือ (Perceived Trust) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ความเชื่อมั่นในระบบปัญญาประดิษฐ์ (Trust in AI) 2) ความไว้วางใจในระบบความปลอดภัยทางไซเบอร์ (Trust in Cyber security) และ 3) ความเชื่อมั่นในโมเดลการเรียนรู้ของเครื่องจักร (Trust in Machine Learning Models)

1.8 ปัจจัยด้านการรับรู้ถึงความง่ายในการใช้ (Perceived Ease of Use) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) การเข้าถึง (Accessibility) 2) ฟังก์ชันการใช้งานที่หลากหลายครอบคลุม (Function) และ 3) ความเข้ากันได้ (Compatibility)

1.9 ปัจจัยด้านการรับรู้ถึงประโยชน์ (Perceived Usefulness) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) การใช้งานระบบมีประสิทธิภาพ (Effective Interfaces) 2) การปรับปรุงสถานะการรักษาความมั่นคงปลอดภัย (Enhanced Cyber Security Posture) และ 3) การลดความเสี่ยงในการถูกโจมตีทางไซเบอร์ (Reducing the risk)

2. การวิเคราะห์โมเดลสมการโครงสร้าง (structural Equation Modeling: SEM)

การวิเคราะห์โมเดลสมการโครงสร้าง ทำให้ทราบความสัมพันธ์ระหว่างตัวแปร เพื่อนำมาวิเคราะห์เส้นทางความสัมพันธ์ระหว่างตัวแปรสังเกตได้ (Observed Variable) และปัจจัยแฝง (latent variable) และเพื่อตรวจสอบความสอดคล้องกลมกลืนระหว่างโมเดลตามสมมติฐานกับข้อมูลเชิงประจักษ์ โดยเกณฑ์ในการตรวจสอบความสอดคล้องกลมกลืนของโมเดลกับข้อมูลเชิงประจักษ์ ผู้วิจัยพิจารณาจากค่าสถิติวัดความกลมกลืน (Goodness of Fit Measures) ซึ่งประกอบด้วยดัชนีดังนี้

2.1 ค่าสถิติไคสแควร์/ค่าชั้นแห่งความเป็นอิสระ (CMIN/df) คือ ดัชนีที่ใช้ในการเปรียบเทียบความกลมกลืนของโมเดลกับข้อมูลเชิงประจักษ์ ค่าไค-สแควร์สัมพัทธ์เป็นการนำค่าไค-สแควร์หารด้วยองศาอิสระ (degrees of freedom : df) เกณฑ์ที่ใช้พิจารณาคือ โมเดลที่มีความสอดคล้องกับข้อมูลเชิงประจักษ์เมื่อค่า (CMIN/df) มีค่าระหว่าง 2.00 ถึง 5.00 ($2.00 \leq x\ 2/df \leq 5.00$) (Bollen, 1989)

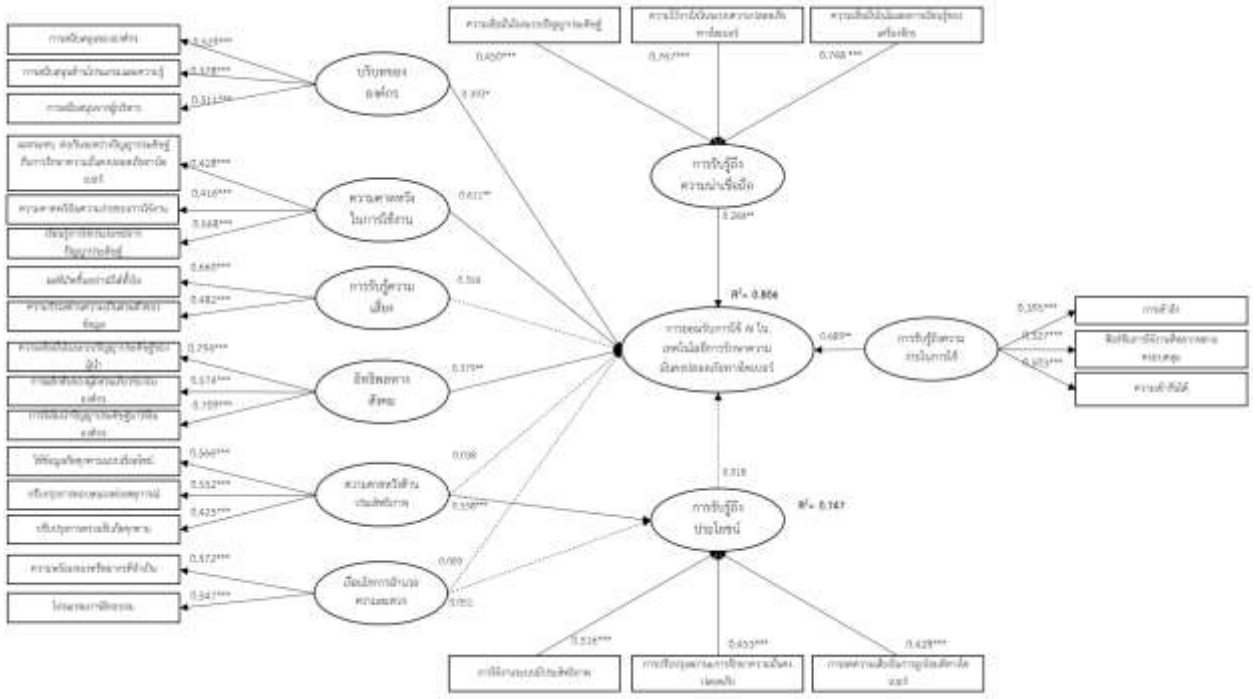
2.2 ค่าดัชนีวัดระดับความสอดคล้อง (Goodness of Fit Index : GFI) เป็นดัชนีที่จัดอยู่ในกลุ่มดัชนีทดสอบความสอดคล้องแบบสัมบูรณ์ (Absolute Fit Index) เป็นค่าที่แสดงถึงปริมาณความแปรปรวนและความแปรปรวนร่วมที่อธิบายได้ด้วยโมเดล โดยค่า GFI จะมีค่าอยู่ระหว่าง 0 และ 1 หากค่า GFI มีค่ามากกว่า 0.90 แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ (Diamantopoulos et al., 2000)

2.3 ค่าดัชนีความกลมกลืนที่ปรับแก้แล้ว (Adjusted Goodness of Fit Index: AGFI) เป็นค่าที่ได้จากการนำดัชนี GFI มาปรับแก้ โดยคำนึงถึงขนาดขององศาอิสระและจำนวนตัวแปร ค่านี้ใช้เกณฑ์เช่นเดียวกับ GFI คือ หากค่า AGFI มีค่ามากกว่า 0.90 แสดงว่าโมเดลมีความสอดคล้องกับข้อมูลเชิงประจักษ์ (Diamantopoulos et al., 2000)

2.4 ดัชนีรากกำลังสองเฉลี่ยของ ความแตกต่างโดยประมาณ (Root Mean Squared Error of Approximation: RMSEA) เป็นค่าสถิติจากข้อตกลงเบื้องต้นเกี่ยวกับ ค่า ไค-สแควร์ว่าโมเดลสมการโครงสร้างตามสมมติฐานมีความเที่ยงตรงนั้นไม่สอดคล้องกับความจริง และเมื่อเพิ่มพารามิเตอร์อิสระและค่าสถิติมีค่าลดลง

เนื่องจากค่าสถิตินี้ขึ้นอยู่กับประชากรและชั้นของความอิสระ RMSEA ควรเท่ากับหรือมีค่าน้อยกว่า 0.05 (Hu and Bentler, 1999)

ผลการวิเคราะห์โมเดลสมการโครงสร้าง พบว่า แบบจำลองมีความสอดคล้องกับข้อมูลเชิงประจักษ์ โดยพิจารณาจากค่า CMIN/df ที่มีค่าเท่ากับ 2.410 ซึ่งอยู่ระหว่าง 2.00 – 5.00 ค่า GFI เท่ากับ 0.936 และค่า AGFI เท่ากับ 0.927 ซึ่งมากกว่า 0.900 และค่า RMSEA มีค่า 0.033 ซึ่งมีค่าไม่เกิน 0.05 เมื่อทำการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรเพื่อทดสอบสมมติฐาน พบว่า ปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ บริบทขององค์กร (Organizational Context) ความคาดหวังในการใช้งาน (Effort Expectancy) อิทธิพลทางสังคม (Social Influence) การรับรู้ถึงความน่าเชื่อถือ (Perceived Trust) และ การรับรู้ถึงประโยชน์ (Perceived Usefulness) ค่าน้ำหนักปัจจัยเท่ากับ 0.393, 0.611, 0.379, 0.244 และ 0.689 ตามลำดับ โดยสามารถอธิบายการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ได้ร้อยละ 80.6 (R^2= .806) ในส่วนปัจจัยที่ส่งผลต่อการรับรู้ถึงประโยชน์ของเทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีปัญญาประดิษฐ์ คือ ปัจจัยด้านความคาดหวังด้านประสิทธิภาพ (Performance Expectancy) ค่าน้ำหนักปัจจัยเท่ากับ 0.558 โดยสามารถอธิบายการรับรู้ถึงประโยชน์ได้ร้อยละ 74.7 (R^2= 0.747) แสดงรายละเอียดดังตารางที่ 1 และภาพที่ 2



CMIN/DF = 2.410, GFI = 0.936, AGFI = 0.927, RMSEA = 0.033

ภาพที่ 2 ผลการวิเคราะห์โมเดลสมการโครงสร้าง

ตารางที่ 1 แสดงผลการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร

ความสัมพันธ์ระหว่างตัวแปร			ค่าน้ำหนักสัมพันธ์มาตรฐาน	P	ผลการทดสอบ
บริบทขององค์กร	--->	การยอมรับการใช้ AI	.393	*	ยอมรับสมมติฐาน
ความคาดหวังในการใช้งาน	--->	การยอมรับการใช้ AI	.611	**	ยอมรับสมมติฐาน
การรับรู้ความเสี่ยง	--->	การยอมรับการใช้ AI	.356	.394	ปฏิเสธสมมติฐาน
อิทธิพลทางสังคม	--->	การยอมรับการใช้ AI	.379	**	ยอมรับสมมติฐาน
ความคาดหวังด้านประสิทธิภาพ	--->	การยอมรับการใช้ AI	-.038	.635	ปฏิเสธสมมติฐาน
เงื่อนไขการอำนวยความสะดวก	--->	การยอมรับการใช้ AI	.009	.898	ปฏิเสธสมมติฐาน
การรับรู้ถึงความน่าเชื่อถือ	--->	การยอมรับการใช้ AI	.244	**	ปฏิเสธสมมติฐาน
การรับรู้ถึงประโยชน์	--->	การยอมรับการใช้ AI	.018	.823	ยอมรับสมมติฐาน
การรับรู้ถึงความง่ายในการใช้	--->	การยอมรับการใช้ AI	.689	**	ยอมรับสมมติฐาน
ความคาดหวังด้านประสิทธิภาพ	--->	การรับรู้ถึงประโยชน์	.558	***	ยอมรับสมมติฐาน
เงื่อนไขการอำนวยความสะดวก	--->	การรับรู้ถึงประโยชน์	.051	.213	ปฏิเสธสมมติฐาน

อภิปรายผล

1. การศึกษาปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สามารถอภิปรายผลการวิจัยได้ดังนี้

1.1 ปัจจัยด้านบริบทขององค์กร ผลการวิจัยพบว่า ปัจจัยด้านบริบทขององค์กรเป็นปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับงานวิจัยของ Dahabiyeh (2021) ที่ทำการศึกษา ปัจจัยที่ส่งผลต่อการยอมรับขององค์กรและการยอมรับเครื่องมือการฝึกอบรมการรับรู้ด้านความปลอดภัยผ่านคอมพิวเตอร์ ผลการศึกษาพบว่า ปัจจัยด้านองค์กรหรือบริบทต่าง ๆ ภายในองค์กรนั้น มีอิทธิพลต่อการยอมรับเครื่องมือการรักษาความมั่นคงปลอดภัยผ่านทางคอมพิวเตอร์ และสอดคล้องกับผลการศึกษาของ ศิริลักษณ์ เมธาธีระนันท์ (2562) ที่พบว่า เกณฑ์การวางนโยบายความปลอดภัยสารสนเทศ ผู้บริหารด้านสารสนเทศ งบประมาณ และการให้ความสำคัญเรื่องความปลอดภัยด้านสารสนเทศ เป็นปัจจัยที่ส่งผลต่อการยอมรับเทคโนโลยีและการปฏิบัติงานจริงของพนักงานผู้ใช้งานของทุกบริษัท

1.2 ปัจจัยด้านความคาดหวังในการใช้งาน ผลการวิจัยพบว่า ปัจจัยด้านความคาดหวังในการใช้งานส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับงานวิจัยของ Ford (2021) ที่ได้ทำการศึกษา ปัจจัยที่มีอิทธิพลต่อการยอมรับเครื่องมือรักษาความปลอดภัยอัจฉริยะเทียมภายในองค์กรเทคโนโลยีสารสนเทศในสหรัฐฯ ผลการศึกษาพบว่า ปัจจัยด้านความคาดหวังในการใช้งานมีอิทธิพลต่อ การยอมรับเครื่องมือรักษาความปลอดภัยอัจฉริยะเทียมภายในองค์กรเทคโนโลยีสารสนเทศในสหรัฐฯ อย่างมีนัยสำคัญทางสถิติ และสอดคล้องกับการศึกษาของ Whittaker and Noteboom (2019) ที่พบว่าความคาดหวังในการใช้งาน มีอิทธิพลเชิงบวกอย่างมีนัยสำคัญต่อความตั้งใจด้านพฤติกรรมในการยอมรับการใช้งานเทคโนโลยี

1.3 ปัจจัยด้านการรับรู้ความเสี่ยง ผลการวิจัยพบว่า ปัจจัยด้านการรับรู้ความเสี่ยงไม่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งขัดแย้งกับงานวิจัยของ Kumar et al. (2023) ที่ทำการศึกษา การรับรู้ความเสี่ยงและความน่าเชื่อถือส่งผลต่อการยอมรับใช้บริการธนาคารบนมือถืออย่างไร หลักฐานเชิงประจักษ์จากอินเดีย ผลการศึกษาพบว่า ปัจจัยด้านการรับรู้ความเสี่ยงไม่มีอิทธิพลต่อพฤติกรรมการใช้งานบริการธนาคารบนมือถือ และขัดแย้งกับ งานวิจัยของ Naw and Kohsuwan (2023) ที่ทำการศึกษาบทบาทของความรู้

ความเสี่ยงที่รับรู้ และความไว้วางใจในการดำเนินการแก้ไขปัญหาความปลอดภัยทางไซเบอร์: การศึกษาในกรุงเทพฯ ประเทศไทย พบว่า การรับรู้ถึงความเสี่ยงของการโจมตีทางไซเบอร์มีบทบาทสำคัญในองค์กร/ธุรกิจในประเทศไทยและความตั้งใจที่จะนำเทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ไปใช้ ทั้งนี้อาจเนื่องมาจากพนักงานผู้ให้ข้อมูลเชื่อว่าองค์กรของตนเองมีความสามารถในการป้องกันการโจมตีและรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพแล้ว ทำให้แม้จะรับรู้ถึงความเสี่ยง แต่ก็ยังมีความเชื่อมั่นในระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอยู่ จึงทำให้การรับรู้ความเสี่ยงไม่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์

1.4 ปัจจัยด้านอิทธิพลทางสังคม ผลการวิจัยพบว่า ปัจจัยด้านอิทธิพลทางสังคมส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับงานวิจัยของ Alneyadi, Kassim and Yin (2022) ที่ทำการศึกษา กรอบแนวคิดเกี่ยวกับปัจจัยที่มีอิทธิพลต่อความตั้งใจของผู้ใช้ในการนำระบบรักษาความปลอดภัยทางไซเบอร์ที่ใช้ AI ไปใช้ในสถานที่ทำงานในประเทศสหรัฐอาหรับเอมิเรตส์ โดยมีการระบุว่า ปัจจัยด้านอิทธิพลทางสังคมนั้นมีอิทธิพลต่อความตั้งใจของผู้ใช้ในการนำระบบรักษาความปลอดภัยทางไซเบอร์ที่ใช้ AI อย่างมีระดับนัยสำคัญทางสถิติ และสอดคล้องกับการศึกษาของ Whittaker and Noteboom (2019) ที่พบว่า การยอมรับและการใช้เทคโนโลยีด้านอิทธิพลทางสังคมมีอิทธิพลเชิงบวกอย่างมีนัยสำคัญต่อความตั้งใจด้านพฤติกรรมในการยอมรับการใช้งานเทคโนโลยี

1.5 ปัจจัยด้านความคาดหวังด้านประสิทธิภาพ ผลการวิจัยพบว่า ปัจจัยด้านความคาดหวังด้านประสิทธิภาพไม่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ แต่มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ของเทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีปัญญาประดิษฐ์อย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับงานวิจัยของ Tanantong and Wongras (2023) ที่ได้ทำการศึกษากรอบการทำงานบนพื้นฐาน UTAUT สำหรับการวิเคราะห์ความตั้งใจของผู้ใช้ในการนำปัญญาประดิษฐ์มาใช้ในการสรรหาบุคลากร: กรณีศึกษาของประเทศไทย ผลการวิจัยพบว่า ปัจจัยด้านความคาดหวังด้านประสิทธิภาพไม่มีอิทธิพลต่อความตั้งใจของผู้ใช้ในการนำปัญญาประดิษฐ์มาใช้ในการสรรหาบุคลากร

1.6 ปัจจัยด้านเงื่อนไขการอำนวยความสะดวก ผลการวิจัยพบว่า ปัจจัยด้านเงื่อนไขการอำนวยความสะดวกไม่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการรับรู้ถึงประโยชน์ของเทคโนโลยี ซึ่งขัดแย้งกับงานวิจัยของ Kumar et al. (2023) ที่ทำการศึกษา การรับรู้ความเสี่ยงและความน่าเชื่อถือส่งผลต่อการยอมรับใช้บริการธนาคารบนมือถืออย่างไร หลักฐานเชิงประจักษ์จากอินเดีย ผลการศึกษาพบว่า ปัจจัยด้านเงื่อนไขการอำนวยความสะดวกมีอิทธิพลต่อการใช้บริการธนาคารบนมือถือ ทั้งนี้อาจเนื่องมาจากในปัจจุบันการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วยเทคโนโลยีอื่น ๆ ต่างก็สามารถอำนวยความสะดวกให้กับผู้ใช้งานได้เหมือน ๆ กัน ส่งผลให้ แม้ว่าเทคโนโลยี AI จะช่วยอำนวยความสะดวกได้ แต่ก็ไม่สามารถทำให้ผู้ใช้งานเกิดการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการรับรู้ถึงประโยชน์ของเทคโนโลยีได้

1.7 ปัจจัยด้านการรับรู้ถึงความน่าเชื่อถือ ผลการวิจัยพบว่า ปัจจัยด้านการรับรู้ถึงความน่าเชื่อถือส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับงานวิจัยของ อคิราภ์ รวมจิตต์ (2564) ที่พบว่า การรับรู้ถึงความน่าเชื่อถือ มีความสัมพันธ์ต่อการยอมรับเทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ของผู้ใช้งาน และสอดคล้องกับการศึกษาของ Naw and Kohsuwan (2023) ที่พบว่า ปัจจัยด้านการรับรู้ถึงความน่าเชื่อถือส่งผลต่อทัศนคติที่ดีต่อระบบป้องกันภัยคุกคาม cyber security solutions ซึ่งทัศนคติที่ดีนั้นมีอิทธิพลให้เกิดพฤติกรรมการตั้งใจใช้งานระบบป้องกันภัยคุกคาม cyber security solutions ได้ จากการทบทวนวรรณกรรมข้างต้นจึงสรุปได้ว่า ปัจจัยทางด้านการรับรู้ถึงความน่าเชื่อถือนั้น มีอิทธิพลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

1.8 ปัจจัยด้านการรับรู้ถึงความง่ายในการใช้ ผลการวิจัยพบว่า ปัจจัยด้านการรับรู้ถึงความง่ายในการใช้ไม่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งขัดแย้งกับงานวิจัยของ Naw and Kohsuwan (2023) ที่ทำการศึกษาบทบาทของความรู้ ความเสี่ยงที่รับรู้ และความไว้วางใจในการดำเนินการแก้ไขปัญหาความปลอดภัยทางไซเบอร์: การศึกษาในกรุงเทพฯ ประเทศไทย พบว่า การรับรู้ถึงประโยชน์และการรับรู้ความง่ายต่อการใช้งานมีบทบาทสำคัญในองค์กร/ธุรกิจในประเทศไทยและความตั้งใจที่จะนำเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้ และขัดแย้งกับการศึกษาของ Hasani et al. (2023) ที่ทำการศึกษาการประเมินการนำความปลอดภัยทางไซเบอร์มาใช้และอิทธิพลที่มีต่อประสิทธิภาพขององค์กร พบว่า ปัจจัยด้านการรับรู้ประโยชน์จากการใช้เทคโนโลยีส่งผลต่อการนำเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้ในองค์กรของพนักงาน ทั้งนี้อาจเนื่องมาจาก เทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับการพัฒนามาในปัจจุบันมีความง่ายในการใช้งานเหมือนกันหมด จึงส่งผลให้แม้ว่าพนักงานผู้ใช้งานจะเกิดการรับรู้ถึงความง่ายในการใช้ แต่ก็ไม่เกิดการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กรได้

1.9 ปัจจัยด้านการรับรู้ถึงประโยชน์ ผลการวิจัยพบว่า ปัจจัยด้านการรับรู้ถึงประโยชน์ มีอิทธิพลทางตรงต่อความตั้งใจใช้เทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีปัญญาประดิษฐ์ อย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับงานวิจัยของ Naw and Kohsuwan (2023) ที่ทำการศึกษาบทบาทของความรู้ ความเสี่ยงที่รับรู้ และความไว้วางใจในการดำเนินการแก้ไขปัญหาความปลอดภัยทางไซเบอร์: การศึกษาในกรุงเทพฯ ประเทศไทย ผลการศึกษาพบว่า การรับรู้ถึงประโยชน์และการรับรู้ความง่ายต่อการใช้งานมีบทบาทสำคัญในองค์กร/ธุรกิจในประเทศไทยและความตั้งใจที่จะนำเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้ ดังนั้นจึงสรุปได้ว่า ปัจจัยการการยอมรับเทคโนโลยี (TAM) มีอิทธิพลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร

2. จากผลการวิเคราะห์ข้อมูลเชิงประจักษ์ด้วยวิธี EFA แสดงให้เห็นว่าโมเดลองค์ประกอบของปัจจัยที่มีผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย 9 ปัจจัยหลัก 25 องค์ประกอบย่อย ดังนี้

2.1 ปัจจัยด้านบริบทขององค์กร (Organizational Context) หลังจากทำการวิเคราะห์เทคนิคปัจจัยเชิงสำรวจ สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ได้ 3 องค์ประกอบ คือ 1) การสนับสนุนขององค์กร (Organization Support) 2) การสนับสนุนด้านโปรแกรมและความรู้ (Program and knowledge Support) และ 3) การสนับสนุนจากผู้บริหาร (Leader Support) กล่าวได้ว่า บุคลากรผู้ใช้งานให้ความสำคัญกับการได้รับการสนับสนุนจากองค์กรทั้งการสนับสนุนในด้านการอบรมให้ความรู้ การสนับสนุนทางนโยบายและวัฒนธรรมองค์กร และการสนับสนุนในด้านวัสดุอุปกรณ์ โครงสร้างพื้นฐานที่จำเป็นต่อการใช้งานเทคโนโลยี เนื่องจาก ผู้ใช้งานมองว่าตนเองเป็นผู้ปฏิบัติงานให้กับองค์กร ผู้บริหารจึงควรให้การสนับสนุนอำนวยความสะดวกในการใช้งาน AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับพนักงาน เพื่อให้พนักงานสามารถเข้าถึงและยอมรับเทคโนโลยีใหม่ ๆ ได้มากยิ่งขึ้น ซึ่งสอดคล้องกับ ศิริลักษณ์ เมธาธีระนันท์ (2562) ที่ได้กล่าวว่า รูปแบบการวางนโยบายความปลอดภัยสารสนเทศ ผู้บริหารด้านสารสนเทศ งบประมาณ โครงสร้างพื้นฐาน และการให้ความสำคัญเรื่องความปลอดภัยด้านสารสนเทศ เป็นปัจจัยสำคัญที่ส่งผลต่อการยอมรับเทคโนโลยีและการปฏิบัติงานจริงของพนักงานผู้ใช้งานของทุกบริษัท (Dahabiyeh, 2021)

2.2 ปัจจัยด้านความคาดหวังในการใช้งาน (Effort Expectancy) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ผลกระทบต่อกันระหว่างปัญญาประดิษฐ์กับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Interacting with AI-driven Cyber security) 2) ความคาดหวังในความง่ายของการใช้งาน (Ease of use) และ 3) เรียนรู้การใช้ประโยชน์จากปัญญาประดิษฐ์ (learning to use AI-powered) กล่าวได้ว่า บุคลากรผู้ใช้งานมีความคาดหวังกับผลกระทบจากการใช้งาน AI เพื่อการรักษาความปลอดภัยเป็นอย่างมาก อีกทั้งยังคาดหวังว่า

AI จะเข้ามาช่วยเหลือให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้นไม่ซับซ้อน มีความง่ายต่อการใช้งานและการเรียนรู้ ซึ่งความคาดหวังในประสิทธิภาพที่ดีของ AI นั้น จะช่วยให้ผู้ใช้งานเกิดการยอมรับในเทคโนโลยีได้มากยิ่งขึ้น สอดคล้องกับ Sair & Danish (2018) ที่ระบุว่า ความคาดหวังถึงความง่ายในการใช้งานและการเรียนรู้เทคโนโลยี AI รวมถึงความคาดหวังในผลเชิงบวกของการใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของผู้ใช้งาน จะช่วยให้ผู้ใช้งานเกิดการยอมรับในเทคโนโลยีนั้นได้มากยิ่งขึ้น(Venkatesh, 2016)

2.3 ปัจจัยด้านการรับรู้ความเสี่ยง (Perceived Risk) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 2 องค์ประกอบ ได้แก่ 1) ผลที่เกิดขึ้นอย่างมิได้ตั้งใจ (Unintended Consequences) และ 2) ความกังวลด้านความเป็นส่วนตัวของข้อมูล (Data Privacy Concerns) กล่าวได้ว่า บุคลกรผู้ใช้งานมีความกังวลในด้านความเป็นส่วนตัวของข้อมูลที่ถูกจัดเก็บและดูแลโดยระบบ AI รวมถึงความกังวลจากผลกระทบจากการใช้งานที่อาจเกิดขึ้นโดยที่ผู้ใช้งานไม่ได้ตั้งใจ หรือผลกระทบที่เกิดขึ้นจากการที่ผู้ใช้งานขาดความรู้ความเข้าใจในระบบ ซึ่งมีผลต่อการยอมรับการใช้เทคโนโลยีของผู้ใช้งาน สอดคล้องกับ ณัฐพร ไชยยากูลวัฒน์ (2560) ที่กล่าวว่า การรับรู้ถึงความไม่แน่นอนจากปัจจัยต่าง ๆ เช่น ปัจจัยทางด้านเทคโนโลยี ปัจจัยด้านการรักษาความปลอดภัย ปัจจัยจากมิจฉาชีพ รวมไปถึงความเสี่ยงที่เกิดจากตัวผู้ใช้งาน เป็นสิ่งที่เกิดขึ้นได้จากการที่บุคลากรได้เรียนรู้หรือทดลองใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

2.4 ปัจจัยด้านอิทธิพลทางสังคม (Social Influence) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ความเชื่อมั่นในระบบปัญญาประดิษฐ์ของผู้นำ (Leaders' confidence in AI) 2) การผลักดันของผู้มีส่วนเกี่ยวข้องในองค์กร (The push in Organizational) และ 3) การริเริ่มนำปัญญาประดิษฐ์มาใช้ในองค์กร (Initiative to use AI in Organizational) กล่าวได้ว่า บุคลากรผู้ใช้งานให้ความสำคัญกับการที่ผู้บริหาร หัวหน้าแผนกหรือหัวหน้าฝ่ายมีการให้ความเชื่อมั่นในระบบ AI จนเกิดมาเป็นการผลักดันองค์กรในมิติต่าง ๆ ให้เกิดการนำเทคโนโลยี AI มาใช้ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ซึ่งปัจจัยดังกล่าวนี้มีผลต่อการยอมรับเทคโนโลยีของผู้ใช้งาน ซึ่งสอดคล้องกับ Song et al. (2018) ที่ได้กล่าวว่า บุคลากรจะเชื่อว่าบุคคลรอบข้าง อาทิเช่น ผู้บริหาร ผู้บังคับบัญชา และเพื่อนร่วมงานมีอิทธิพลต่อตนเอง อีกทั้งผู้ใช้งานจะเชื่อว่าตนเองต้องปฏิบัติตามคนรอบข้าง ดังนั้นหากผู้บริหารและผู้บังคับบัญชามีการผลักดันและริเริ่มการใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ก็จะส่งผลให้บุคลากรภายในองค์กรเกิดการยอมรับและใช้งานตามไปด้วย (Kassim and Yin, 2022)

2.5 ปัจจัยด้านความคาดหวังด้านประสิทธิภาพ (Performance Expectancy) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ให้ข้อมูลภัยคุกคามแบบเรียลไทม์ (Provide real-time threat intelligence) 2) ปรับปรุงการตอบสนองต่อเหตุการณ์ (Enhanced incident response) และ 3) ปรับปรุงการตรวจจับภัยคุกคาม (Improved threat detection) กล่าวได้ว่า บุคลากรผู้ใช้งานมีความคาดหวังในประสิทธิภาพในการให้ข้อมูลภัยคุกคามได้แบบเรียลไทม์ และมีการวิเคราะห์ ประมวลผลเพื่อหาวิธีการรับมือและตรวจจับภัยคุกคามได้ด้วยตนเอง โดยที่ไม่ต้องมีมนุษย์เป็นคนคอยควบคุม ซึ่งสอดคล้องกับ Venkatesh et al. (2016) ที่กล่าวว่าความคาดหวังว่าการใช้ระบบสารสนเทศจะช่วยให้ความสามารถในการปฏิบัติงานดีขึ้นหรือเชื่อมั่นว่าการใช้ระบบสารสนเทศจะช่วยให้ได้รับประโยชน์ในการทำงาน เป็นความคาดหวังในประสิทธิภาพการทำงานของ AI ในการรักษาความมั่งคงปลอดภัยทางไซเบอร์ (Ford, 2021)

2.6 ปัจจัยด้านเงื่อนไขการอำนวยความสะดวก (Facilitating Conditions) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 2 องค์ประกอบ ได้แก่ 1) ความพร้อมของทรัพยากรที่จำเป็น (Availability of necessary resources) และ 2) โปรแกรมการฝึกอบรม (Presence of training programs) กล่าวได้ว่า บุคลากรผู้ใช้งานมีการให้ความสำคัญกับความพร้อมของโครงสร้างพื้นฐานภายในองค์กร เช่น ฮาร์ดแวร์ ซอฟแวร์ ระบบเครือข่ายอินเตอร์เน็ตที่จำเป็นต่อการใช้งานเทคโนโลยี AI และให้ความสำคัญกับโปรแกรมการฝึกอบรม การให้ความรู้ความเข้าใจแก่บุคลากรเกี่ยวกับการใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นอย่างมาก เนื่องจากทรัพยากร

พื้นฐานที่จำเป็นและความรู้ความเข้าใจในระบบเป็นสิ่งสำคัญต่อการใช้งานเทคโนโลยีที่มีประสิทธิภาพ ซึ่งสอดคล้องกับ Venkatesh et al. (2016) ที่กล่าวว่า โครงสร้างพื้นฐานด้านเทคนิคและการอบรมให้ความรู้เป็นปัจจัยที่จะช่วยสนับสนุนให้บุคลากรสามารถใช้งานระบบเทคโนโลยีใหม่ได้อย่างมีประสิทธิภาพ ซึ่งปัจจัยที่กล่าวไปนั้นส่งผลต่อความเชื่อของผู้ใช้งานเกี่ยวกับสิ่งอำนวยความสะดวกที่มีอยู่ (Rad et al., 2014)

2.7 ปัจจัยด้านการรับรู้ถึงความน่าเชื่อถือ (Perceived Trust) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) ความเชื่อมั่นในระบบปัญญาประดิษฐ์ (Trust in AI) 2) ความไว้วางใจในระบบความปลอดภัยทางไซเบอร์ (Trust in Cyber security) และ 3) ความเชื่อมั่นในโมเดลการเรียนรู้ของเครื่องจักร (Trust in Machine Learning Models) กล่าวได้ว่า บุคลากรผู้ใช้งานให้ความสำคัญกับความน่าเชื่อถือในปัญญาประดิษฐ์ว่าจะมีระบบการรักษาความปลอดภัยและโมเดลการเรียนรู้ที่มีประสิทธิภาพ เหมาะสมกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กร ซึ่งสอดคล้องกับ กษมา จินุกูล (2562) ที่ได้กล่าวว่า ความน่าเชื่อถือเป็นระดับความมั่นใจหรือความไว้ใจในระบบการบริการของผู้ให้บริการว่ามีประสิทธิภาพและสามารถให้บริการได้อย่างมีมาตรฐาน อันส่งผลให้เกิดประโยชน์แก่ผู้ใช้งานได้ ซึ่งความน่าเชื่อถือของระบบมีความสัมพันธ์กับการยอมรับเทคโนโลยีของผู้ใช้งาน

2.8 ปัจจัยด้านการรับรู้ถึงความง่ายในการใช้ (Perceived Ease of Use) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) การเข้าถึง (Accessibility) 2) ฟังก์ชันการใช้งานที่หลากหลาย ครอบคลุม (Function) และ 3) ความเข้ากันได้ (Compatibility) กล่าวได้ว่า บุคลากรผู้ใช้งานให้ความสำคัญกับความง่ายในการเข้าใช้งานระบบ และความยืดหยุ่นในการเข้าใช้งาน ที่สามารถเข้าใช้งานได้ทุกที่ ทุกเวลา จากระบบปฏิบัติการที่แตกต่างกันภายในองค์กร รวมถึงการมีฟังก์ชันการใช้งานที่สามารถใช้งานได้จริง มีความหลากหลาย และเหมาะสมต่อการนำมาใช้ในระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กร สอดคล้องกับ Hanif and Lallie (2021) ที่ได้กล่าวไว้ว่า การรับรู้ความง่ายในการใช้งานถูกอธิบายด้วยความคาดหวังของผู้ใช้งานระบบเทคโนโลยีว่าเป็นระบบที่สะดวกสบายในการเข้าถึง สามารถใช้งานได้ง่าย มีความหลากหลายและครอบคลุมในทุกความต่างของอุปกรณ์ที่เข้าใช้งาน

2.9 ปัจจัยด้านการรับรู้ถึงประโยชน์ (Perceived Usefulness) สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบใหม่ คือ 3 องค์ประกอบ ได้แก่ 1) การใช้งานระบบมีประสิทธิภาพ (Effective Interfaces) 2) การปรับปรุงสถานะการรักษาความมั่นคงปลอดภัย (Enhanced Cyber Security Posture) และ 3) การลดความเสี่ยงในการถูกโจมตีทางไซเบอร์ (Reducing the risk) กล่าวได้ว่า บุคลากรผู้ใช้งาน กล่าวได้ว่า การรับรู้ประโยชน์เป็นระดับกระบวนการรับรู้ที่ผู้ใช้งานเชื่อมั่นว่าประโยชน์ของเทคโนโลยี AI จะสามารถปรับปรุงสถานะในการดำเนินงานให้มีประสิทธิภาพและตอบสนองความต้องการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กรได้รวมถึงจะช่วยลดความเสี่ยงในการโจมตีทางไซเบอร์ที่อาจเกิดขึ้น (Yang et al., 2020)

ข้อเสนอแนะ

ข้อเสนอแนะในการนำผลการวิจัยไปประยุกต์ใช้

1. สำหรับผู้บริหารองค์กร ควรให้ความสำคัญกับการสนับสนุนขององค์กรทั้งในด้านโปรแกรมและให้ความรู้เกี่ยวกับการใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการวางแผนนโยบาย โครงสร้างพื้นฐานภายในองค์กร และสร้างวัฒนธรรมองค์กรในรูปแบบใหม่ที่เอื้อต่อการใช้งานเทคโนโลยี AI เพื่อสร้างความพร้อมและความสามารถในการใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรภายในองค์กรได้อย่างมีประสิทธิภาพ

2. สำหรับผู้พัฒนาเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ควรพัฒนาเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพและมีความสามารถที่เป็นเอกลักษณ์และน่าสนใจกว่าคู่แข่งขัน อาทิเช่น การพัฒนาขีดความสามารถในการตรวจจับการบุกรุกให้ทำงานได้อย่างรวดเร็ว การพัฒนาให้ระบบ

สามารถสร้างรูปแบบการป้องกันการโจมตีได้ด้วยการประมวลผลของตนเอง อีกทั้งยังควรให้ความสำคัญกับการกระตุ้นให้ผู้ใช้งานรับรู้ถึงความง่ายในการใช้งาน และประโยชน์จากกงานใช้งานเทคโนโลยี AI ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดียิ่งกว่าเทคโนโลยีแบบเดิม เพื่อให้ผู้ใช้งานเกิดการรับรู้ถึงความเหนือกว่าของเทคโนโลยี AI และเกิดการยอมรับและใช้งานเทคโนโลยีในเวลาต่อมาได้

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

1. สำหรับงานวิจัยในครั้งถัดไป ควรมีการเก็บแบบสอบถามในหน่วยงานของภาคอุตสาหกรรมอื่น ๆ เพื่อเป็นการยืนยันปัจจัยที่ส่งผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ว่ามีความสอดคล้องกับผลการศึกษาในครั้งนี้หรือไม่ และเพื่อนำผลการศึกษามาพัฒนากลยุทธ์ในการสร้างการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของพนักงานในองค์กร อย่างเหมาะสมและมีประสิทธิภาพ

2. ควรมีการศึกษาเพิ่มเติมในมิติของตัวแปรอื่น ๆ ที่อาจมีผลต่อการยอมรับการใช้ AI ในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรได้ เช่น ปัจจัยส่วนบุคคล นโยบายองค์กร ความรู้ความเข้าใจในการใช้งานเทคโนโลยี ทัศนคติต่อการใช้งาน เป็นต้น เพื่อผลการศึกษาที่ครอบคลุมและแหลากหลายมากยิ่งขึ้น

เอกสารอ้างอิง

กษมา จินุกุล. (2562). *การรับรู้ความเสี่ยงและความไว้วางใจที่ส่งผลต่อความตั้งใจในการทำธุรกรรมทางการเงินผ่านธนาคารบนมือถือของลูกค้าธนาคารกรุงไทย จำกัด (มหาชน) ในจังหวัดสงขลา*. วิทยานิพนธ์บริหารธุรกิจมหาบัณฑิต สาขาวิชาการตลาด มหาวิทยาลัยสงขลา.

โกศล จิตวิรัตน์. (2561). โมเดลการปรับตัวขององค์การธุรกิจที่ได้รับผลกระทบจากการทำลายล้างของเทคโนโลยีดิจิทัลในศตวรรษที่ 21. *วารสารสมาคมนักวิจัย*, 23(2), 74–88.

ณัฐ เลิศฤทธิ์. (2560). *การประเมินแผนบริหารความต่อเนื่องทางธุรกิจ บริษัท ไปรษณีย์ไทย จำกัด ในภาวะประสบอุทกภัยและสภาวะวิกฤตในเขตกรุงเทพมหานคร*. การค้นคว้ารัฐศาสตรมหาบัณฑิต สาขาวิชารัฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

ณัฐพร ไชยยากูลวัฒน์. (2560). *การประยุกต์ทฤษฎีรวมการยอมรับและใช้เทคโนโลยีเพื่อเข้าใจการ ยอมรับชุมชนการลงทุนเสมือนของนักลงทุนรายย่อย*. การค้นคว้าอิสระบริหารธุรกิจมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยกรุงเทพ.

ปาริฉัตร วิชุภากรณ์กุล. (2563). *การเตรียมความพร้อมต่อการเปลี่ยนแปลงสู่เทคโนโลยีปัญญาประดิษฐ์ของพนักงานโรงแรมใน กรุงเทพมหานคร*. วิทยานิพนธ์บริหารธุรกิจมหาบัณฑิต หลักสูตรบริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยศิลปากร.

ศิริลักษณ์ เมธาธีระนันท์. (2562*). การศึกษาภัยคุกคามทางไซเบอร์ จากช่องว่างระหว่างการวางนโยบายความปลอดภัยสารสนเทศกับการใช้งานจริงของพนักงานในองค์กร กรณีศึกษา บริษัทญี่ปุ่นในประเทศไทย*. การค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต สาขาวิชานโยบายและการบริหารดิจิทัล มหาวิทยาลัยธรรมศาสตร์.

สุรพงษ์ คงสัตย์ และ ธีรชาติ ธรรมวงค์ (2558). *การหาค่าความเที่ยงตรงของแบบสอบถาม (IOC)*. มหาวิทยาลัยมหาจุฬาลงกรณ์ราชวิทยาลัย. https://www.mcu.ac.th/article/detail/14329

อมรรักษ์ สวนชูผล. (2563). การจัดการธุรกิจการบริการผู้สูงอายุ. *วารสารวิจัยและพัฒนา วไลยอลงกรณ์ ในพระบรมราชูปถัมภ์*, 13(1), 146–152.

อรพรรณ คงมาลัย และอัญณิฐา ดิษฐานนท์. (2562). *เทคนิควิจัยด้านการบริหารเทคโนโลยีและนวัตกรรม*. มหาวิทยาลัยธรรมศาสตร์.

Reference

Abrahão, R.S. (2016). Intention of adoption of mobile payment: An analysis in RAI. *Revista de Administração e Inovação, 13*(3), 221–230.

Alneyadi, M. R. M. A. H., Md Kassim, N., & Yin, T. S. (2022). Conceptual framework on the factors influencing users' intention to adopt AI-based cybersecurity systems at workplaces in the UAE. *Global Business & Management Research, 14*(3), 1053–1064.

Bollen, K. A. (1989). A new incremental fit index for general structural equation models. *Sociological Methods and Research, 17*(3), 303–316.

Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security, 29*(5), 836–849.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.

Diamantopoulos, A., Siguaw, J. A., and Cadogan, J. W. (2000). *Export peformance: The impact of cross-country export market orientation*. Paper presented at the American Marketing Association. Conference Proceedings.

Diamantopoulos, A., Siguaw, J. A., & Cadogan, J. W. (2000). Export performance: The impact of cross-country export market orientation. In *Marketing theory and applications: Proceedings of the American Marketing Association Winter Conference*. (Vol. 11, pp. 177–178). American Marketing Association.

Dwivedi, Y. K., Rana, N. P., Janssen, M., Lal, B., Williams, M. D., & Clement, M. (2017). An empirical validation of a unified model of electronic government adoption (UMEGA). *Government Information Quarterly, 34*(2), 211–230.

Field, A. (2017). *Discovering statistics using IBM SPSS Statistics* (5th ed.). SAGE Edge.

Ford, C. (2021). *Factors influencing the acceptance of artificially intelligent security tools within US-based information technology organizations*. Doctoral dissertation, University of the Cumberlands.

Hair, J. F., Balck, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A global perspective* (7th ed.). Pearson.

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM with perceived cyber security, risk, and trust. *Technology in Society, 67*(1), 1–14.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics, 3*(5), 97–135.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Kumar, R., Singh, R., Kumar, K., Khan, S., & Corvello, V. (2023). How does perceived risk and trust affect mobile banking adoption? Empirical evidence from India. *Sustainability, 15*(5), 4053–4074.

Lindeman, P., & Shea, J. J. (1980). Size of the mastoid air cell system in children with middle ear effusion. *The Laryngoscope, 90*(11), 1840–1844.

Naw, T. D., & Kohsuwan, P. (2023). Roles of perceived knowledge, risk, and trust in cybersecurity solution implementation: A study in Bangkok, Thailand. *Human Behavior, Development & Society, 24*(3), 81–92.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

Rad, M. S., Dahlan, H. M., Iahad, N. A., Nilashi, M., & Zakaria, R. (2014). Assessing the factors that affect adoption of social research network site for collaboration by researchers using multi-criteria approach. *Journal of Theoretical & Applied Information Technology, 65*(1), 170–182.

Sair, S. A., & Danish, R. Q. (2018). Effect of performance expectancy and effort expectancy on the mobile commerce adoption intention through personal innovativeness among Pakistani consumers. *Pakistan Journal of Commerce Social Sciences, 12*(2), 501–520.

Song, J., Baker, J., Wang, Y., Choi, H. Y., & Bhattacherjee, A. (2018). Platform adoption by mobile application developers: A multimethodological approach. *Decision Support Systems, 107*(4), 26–39.

Tanantong, T., & Wongras, P. (2024). A UTAUT-based framework for analyzing users' intention to adopt artificial intelligence in human resource recruitment: A case study of Thailand. *Systems, 12*(1), 28–35.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the association for Information Systems, 17*(5), 328–376.

Whittaker, T. A., & Noteboom, C. (2019). Factors influencing curriculum adoption in undergraduate cybersecurity programs. *Issues in Information Systems, 20*(3), 63–73.

Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management, 28*(1), 167–183.

คณะผู้เขียน

ศุภวัฒน์ เคหาบาล

วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์

เลขที่ 2 ถนนพระจันทร์ แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพมหานคร 10200

email: supawat.khe@dome.tu.ac.th

จิโรจน์ บุรณศิริ

วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์

เลขที่ 2 ถนนพระจันทร์ แขวงพระบรมมหาราชวัง เขตพระนคร กรุงเทพมหานคร 10200

email: jiroj@tu.ac.th