ปีที่ 7 ฉบับที่ 2: กรกฎาคม - ธันวาคม 2564
Volume 7 Number 2: July - December 2021

แนวทางปฏิบัติที่ดีสำหรับหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์: กรณีศึกษาของโรงเรียนนายร้อยตำรวจ

A Good Practice for Cybersecurity Teaching Curriculum: A Case Study of The Royal Police Cadet Academy

วงศ์ยศ เกิดศรี
คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

Wongyos Keardsri
Faculty of Forensic Science, Royal Police Cadet Academy

Received July 3, 2021 | Revised December 17, 2021 | Accepted December 20, 2021

บทความวิจัย (Research Article)

บทคัดย่อ

บทความเรื่องนี้เป็นการวิจัยเชิงออกแบบ ทดลอง และพัฒนา แนวทางปฏิบัติที่ดีสำหรับหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นหลักสูตรพิเศษเฉพาะทางสำหรับการเรียนการสอนของโรงเรียนนายร้อยตำรวจ ปัจจุบันหลักสูตรการศึกษาสำหรับนักเรียนนายร้อยตำรวจนั้นเป็นหลักสูตรทางด้านรัฐประศาสนศาสตร์ ซึ่งยังคงมีวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ไม่เพียงพอ ดังนั้นการศึกษาวิจัยเรื่องนี้จึงมีวัตถุประสงค์สำคัญเพื่อส่งเสริมและพัฒนาต้นแบบหลักสูตรการเรียนการสอนใหม่ ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับนักเรียนนายร้อยตำรวจ เพื่อให้มีองค์ความรู้ที่เพียงพอกับการปฏิบัติหน้าที่ในคดีอาชญากรรมไซเบอร์เมื่อสำเร็จการศึกษา โครงสร้างของหลักสูตรแบ่งออกเป็น 2 ส่วน ได้แก่ 1) การศึกษาความรู้พื้นฐานด้านวิทยาการคอมพิวเตอร์ที่จำเป็นสำหรับการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และ 2) การศึกษาความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งยังสามารถแบ่งออกเป็นความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์เชิงรุกที่ประกอบไปด้วย การเขียนโปรแกรมสำหรับการแฮ็กอย่างมีจรรยาบรรณ การเข้าถึงทรัพยากรของเครือข่ายและเครื่อง การเข้าถึงทรัพยากรของเว็บ และการยึดครอง และ ความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์เชิงรับ ที่ประกอบไปด้วย การทำวิศวกรรมย้อนกลับ การตรวจพิสูจน์ทางดิจิทัล วิทยาการเข้ารหัสลับ และการประยุกต์ใช้เครื่องมือโอเอสไอเอ็นที การจัดกิจกรรมการเรียน การสอนจะเป็นรูปแบบการเรียนรู้ผ่านเกมที่เรียกว่าซีทีเอฟหรือการยึดธง ผลการศึกษาพบว่านักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมีทักษะด้านความมั่นคงปลอดภัยไซเบอร์หลังผ่านการเรียนการสอนในหลักสูตรดังกล่าวเพิ่มขึ้นอย่างมีนัยสำคัญ และสามารถสร้างผลงานและแสดงศักยภาพทางด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ได้ ทั้งในระดับเหล่าทัพ ระดับชาติ และระดับนานาชาติ

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์, การเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์, หลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์, โรงเรียนนายร้อยตำรวจ

Abstract

This article is a research study for designing, experimenting, and developing a good practice of teaching curriculum in cybersecurity, which is a special course for the teaching of the Royal Police Cadet Academy. Currently, the education program for police cadets is in public administration. There are still not enough courses related to cybersecurity. Therefore, this research has an important objective to promote and develop a new teaching model and learning curriculum in cybersecurity for police cadets to have sufficient knowledge for performing their duties in cybercrime cases after graduation. The course structure is divided into two parts: 1) the study of necessary knowledge of computer science for cybersecurity learning, and 2) the study of cybersecurity principles, which can also be divided into the knowledge of offensive cybersecurity which consists of programming for ethical hacking, network and machine exploitation, web exploitation and pwnable, and the knowledge of defensive cybersecurity that consists of reverse engineering, digital forensic, cryptography and the application of OSINT tools. The teaching activities will be game-based learning which is called CTF or capture the flag. The research study found that the samples of police cadets have significantly increased their cybersecurity skills after completing the course and they can show the performance and potential in cybersecurity at the military, national, and international levels.

Keywords: Cybersecurity, Cybersecurity Learning**,** Cybersecurity Curriculum, Royal Police Cadet Academy

บทนำ

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) เป็นองค์ความรู้หนึ่งที่มีความสำคัญอย่างมากสำหรับนักเรียนนายร้อยตำรวจยุคใหม่ที่จะต้องนำไปใช้ในการปฏิบัติงานจริงเมื่อสำเร็จการศึกษาจากโรงเรียนนายร้อยตำรวจ ปัจจุบันพบว่ารูปแบบของอาชญากรรมนั้นเปลี่ยนไปจากเดิมจากอาชญากรรมตามท้องถนน (Street Crime) เป็นอาชญากรรมทางไซเบอร์ (Cybercrime) แต่นักเรียนนายร้อยตำรวจนั้นยังคงมีความรู้ที่ไม่เพียงพอในการรับมือกับอาชญากรรมทางไซเบอร์รูปแบบใหม่นี้อย่างครบถ้วนสมบูรณ์ ทั้งยังไม่เข้าใจในหลักการทางเทคนิคเชิงลึกที่จะต้องนำไปใช้ในการสืบสวนหาร่องรอยและหาตัวของคนร้ายในโลกไซเบอร์ได้อย่างมีประสิทธิภาพ

หลักสูตรรัฐประศาสนศาสตรบัณฑิต สาขาวิชาการตำรวจ โรงเรียนนายร้อยตำรวจ (2018) ซึ่งเป็นหลักสูตรปรับปรุง พ.ศ.2561 นั้น ได้กำหนดวิชาเรียนที่เกี่ยวข้องกับเนื้อหาทางด้านวิทยาการคอมพิวเตอร์และความมั่นคงปลอดภัยไซเบอร์ไว้จำนวน 3 วิชา ได้แก่ วิชาเทคโนโลยีดิจิทัลสำหรับการบริหารงานตำรวจเป็นวิชาหมวดศึกษาทั่วไปของนักเรียนนายร้อยตำรวจชั้นปีที่ 1 วิชาอาชญากรรมคอมพิวเตอร์ เป็นวิชาหมวดวิชาเฉพาะของนักเรียนนายร้อยตำรวจชั้นปีที่ 3 และวิชาความมั่นคงปลอดภัยไซเบอร์ เป็นวิชาหมวดเลือกเสรีของนักเรียนนายร้อยตำรวจชั้นปีที่ 4 ซึ่งยังคงไม่เพียงพอในการเรียนการสอนทางด้านความมั่นคงปลอดภัยทางไซเบอร์ของนักเรียนนายร้อยตำรวจในยุคปัจจุบัน ดังนั้นจึงมีความจำเป็นต้องปรับปรุง

หลักสูตรให้ทันสมัยและสอดรับกับรูปแบบอาชญากรรมที่เปลี่ยนไปเป็นอาชญากรรมทางไซเบอร์ให้มากยิ่งขึ้น ผู้วิจัยได้ริเริ่มโครงการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการเตรียมความพร้อมในด้านทักษะและองค์ความรู้ทางไซเบอร์ให้กับนักเรียนนายร้อยตำรวจเป็นประจำทุกปี ตั้งแต่ปี พ.ศ. 2561 เป็นต้นมา ทั้งนี้เพื่อเป็นการฝึกอบรมให้นักเรียนนายร้อยตำรวจมีองค์ความรู้พื้นฐานขั้นต้น ขั้นกลาง และขั้นสูงทางด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งคัดเลือกนักเรียนนายร้อยตำรวจเพื่อเป็นตัวแทนของโรงเรียนนายร้อยตำรวจเข้าร่วมการแข่งขันทักษะทางไซเบอร์ระดับเหล่าทัพ ระดับชาติ และระดับนานาชาติ โดยผลสัมฤทธิ์จากการฝึกอบรมแสดงให้เห็นถึงพัฒนาการของนักเรียนนายร้อยตำรวจในด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีนัยสำคัญและเป็นที่น่าพอใจอย่างยิ่ง

ดังนั้นการศึกษาวิจัยเรื่องนี้จึงต้องการนำเสนอแนวทางปฏิบัติที่ดี (Good Practice) ในเรื่องหลักสูตรการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์แก่นักเรียนนายร้อยตำรวจ ทั้งนี้เพื่อใช้เป็นต้นแบบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโรงเรียนนายร้อยตำรวจต่อไป และทั้งยังเป็นต้นแบบและแนวทางปฏิบัติที่ดีสำหรับหน่วยงานทางด้านการศึกษาที่มีการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยและนานาชาติอีกด้วย

วัตถุประสงค์

1) เพื่อออกแบบ ทดลอง และพัฒนา แนวทางปฏิบัติที่ดี ที่เป็นต้นแบบหลักสูตรการเรียนการสอนแบบใหม่ทางด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโรงเรียนนายร้อยตำรวจ

2) เพื่อส่งเสริมและพัฒนาองค์ความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ที่เพียงพอให้กับนักเรียนนายร้อยตำรวจในการปฏิบัติหน้าที่ในคดีทางอาชญากรรมไซเบอร์เมื่อสำเร็จการศึกษา

3) เพื่อสร้างผลงานและแสดงศักยภาพทางด้านความมั่นคงปลอดภัยไซเบอร์ของโรงเรียนนายร้อยตำรวจให้เป็นที่ประจักษ์ทั้งในระดับเหล่าทัพ ระดับชาติ และระดับนานาชาติ

กรอบแนวคิดการวิจัย

การศึกษาวิจัยเรื่องนี้มีกรอบแนวคิดเพื่อใช้ในการออกแบบ ทดลอง และพัฒนา แนวทางปฏิบัติที่ดีของหลักสูตรการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ โดยเริ่มต้นจากการศึกษาขอบเขตและรายละเอียดของหลักสูตรทางด้านความมั่นคงปลอดภัยไซเบอร์ จากนั้นจึงได้ออกแบบหลักสูตรการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ ตามด้วยการคัดเลือกกลุ่มตัวอย่างสำหรับการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ การทดลองและติดตามผลกิจกรรมการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ และการสรุปผลและอภิปรายผล โดยมีรายละเอียดดังแสดงตามภาพที่ 1

ภาพที่ 1 แนวทางและกรอบแนวคิดในการวิจัย

ทบทวนวรรณกรรม

1) หลักสูตรการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์

จากการศึกษาขอบเขตและสำรวจหลักสูตรที่เกี่ยวข้องกับการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทยนั้นพบว่า หลักสูตรส่วนใหญ่เป็นหลักสูตรในระดับบัณฑิตศึกษาที่เป็นระดับปริญญาโทและปริญญาเอก ในขณะที่หลักสูตรในระดับปริญญาตรีนั้นเป็นเพียงการสอดแทรกรายวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ไว้ในหลักสูตรปัจจุบันที่มีการเรียนการสอนอยู่เดิม โดยผู้วิจัยได้สำรวจโครงสร้างของหลักสูตรแบบเชิงลึกทั้งในส่วนของชื่อวิชา คำอธิบายรายวิชา และเอกสารประกอบการสอนรายวิชา ของหลักสูตรในระดับปริญญาตรี 3 หลักสูตร ซึ่งมีรายละเอียดดังต่อไปนี้

(1) หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย (2018) มีรายวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์คือ วิชาความมั่นคงของคอมพิวเตอร์ (Computer Security) ซึ่งมีเนื้อหาที่เกี่ยวข้องกับหลักการของความมั่นคงของคอมพิวเตอร์ วิทยาการเข้ารหัสลับแบบกุญแจสมมาตร วิทยาการเข้ารหัสลับแบบกุญแจสาธารณะ การย่อยสาร การพิสูจน์ตัวจริง การควบคุมการเข้าถึง ความมั่นคงของวิสาหกิจ และความมั่นคงของเครือข่าย

(2) หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร (นานาชาติ) มหาวิทยาลัยมหิดล (2018) มีรายวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์คือ วิชาความมั่นคงของคอมพิวเตอร์และการสื่อสาร (Computer and Communication Security) ซึ่งมีเนื้อหาที่เกี่ยวข้องกับระบบความปลอดภัย การเข้ารหัส การวิเคราะห์รหัส มาตรฐานการเข้ารหัสข้อมูล เทคนิคการสร้างรหัสและข้อตกลงในการสื่อสาร การประยุกต์ใช้รหัสในการจัดการระบบรหัสสาธารณะ ลายเซ็นแบบดิจิตอล ระบบความปลอดภัยของแฟ้มข้อมูล และการเข้าไปในระบบฐานข้อมูล และ วิชาการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ซึ่งมีเนื้อหาที่เกี่ยวข้องกับการพิสูจน์ข้อมูลในฮาร์ดดิสต์ การพิสูจน์หลักฐานบนระบบเครือข่าย การพิสูจน์หลักฐานอีเมลและอินเทอร์เน็ต และ การรวบรวมหลักฐานแบบทันท่วงทีบนระบบปฏิบัติการ

(3) หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ประยุกต์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี (2017) ซึ่งมีรายวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์คือ วิชาความมั่นคงทางไซเบอร์ (Cybersecurity) ซึ่งมีเนื้อหาที่เกี่ยวข้องกับหลักการพื้นฐานของความมั่นคง หลักการการออกแบบความมั่นคง ภัยคุกคามและการโจมตี การเขียนโปรแกรมเชิงป้องกัน ความมั่นคงทางเครือข่าย วิทยาการเข้ารหัสลับ ความมั่นคงทางเว็บ ความมั่นคงทางแพลตฟอร์ม นโยบายความมั่นคง วิศวกรรมซอฟต์แวร์เพื่อความมั่นคง และวิศวกรรมย้อนกลับ

จากการสำรวจขอบเขตของเนื้อหารายวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของทั้ง 3 หลักสูตรข้างต้นนั้นพบว่า มีรายละเอียดที่สอดคล้องกัน โดยประกอบไปด้วยเนื้อหาที่สำคัญ ได้แก่ มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ ความมั่นคงทางเครือข่ายคอมพิวเตอร์ ความมั่นคงทางแพลตฟอร์ม ความมั่นคงทางเว็บ วิทยาการเข้ารหัสลับ วิศวกรรมย้อนกลับ และการตรวจพิสูจน์ทางดิจิทัล

2) งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องในช่วง 5 ปีที่ผ่านมานั้นได้มีการกำหนดแนวทางและขอบเขตเนื้อหาในหลักสูตรการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ไว้หลากหลาย ผู้วิจัยขอยกตัวอย่างงานวิจัยที่น่าสนใจดังต่อไปนี้ Peruma et al. (2018) ได้กล่าวถึงปัญหาการขาดแคลนผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจำเป็นจะต้องได้รับการฝึกอบรมเพิ่มขึ้นเพื่อสร้างบุคลากรทางด้านนี้ให้เพียงพอกับ

ความต้องการ โดยงานวิจัยเรื่องนี้ได้นำเสนอห้องปฏิบัติการทางด้านความปลอดภัยไซเบอร์บนแอปพลิเคชันมือถือ ซึ่งเปิดเป็นสาธารณะให้บุคคลทั่วไปสามารถเข้าใช้งานและเรียนรู้ได้ ในขณะที่ Omar et al. (2018) ได้กล่าวถึงกระบวนการเตรียมหลักสูตรการเรียนการสอนในระดับปริญญาตรีทางด้านความมั่นคงปลอดภัยไซเบอร์ โดยจะต้องประกอบไปด้วยขั้นตอนการศึกษาโครงสร้างของหลักสูตร การออกแบบและวิเคราะห์หลักสูตร และการใช้งานหลักสูตร ทั้งนี้วิชาเรียนในหลักสูตรนั้นจะต้องประกอบไปด้วยเนื้อหาขั้นพื้นฐาน ขั้นกลาง และขั้นสูง ที่ผู้เรียนสามารถนำไปประยุกต์ใช้งานจริงเมื่อสำเร็จการศึกษา งานวิจัยดังกล่าวสอดคล้องกับงานวิจัยของ Dai (2019) ที่กล่าวถึงความสำคัญของหลักสูตรการเรียนการสอนและการใช้เครื่องมือทางด้านความมั่นคงปลอดภัยไซเบอร์ที่จะต้องมีความหลากหลายและสอดรับกับสถานการณ์ทางด้านภัยคุกคามทางไซเบอร์ในปัจจุบัน ในขณะที่งานวิจัยของ Crick et al. (2019) ได้กล่าวถึงกรณีศึกษาของหลักสูตรทางด้านความมั่นคงปลอดภัยไซเบอร์ในสหราชอาณาจักรที่พยายามปรับความรู้เชิงทฤษฎีไปสู่การปฏิบัติมากยิ่งขึ้น เนื่องจากองค์ความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์นั้น จำเป็นจะต้องได้รับการฝึกปฏิบัติจากสถานการณ์จริง งานวิจัยของ Yuan et al. (2019) ได้กล่าวเพิ่มเติมว่าการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์นั้น จำเป็นจะต้องสอดแทรกเนื้อหาทางด้านการสื่อสาร ทัศนคติ การทำงานเป็นทีม การสร้างเครือข่าย การแก้ปัญหา และการคิดอย่างมีวิจารณญาณ เนื่องจากผู้ที่ปฏิบัติหน้าที่ทางด้านความมั่นคงปลอดภัยไซเบอร์จะต้องมีการบูรณาการข้อมูลซึ่งกันและกันอยู่ตลอดเวลา นอกเหนือจากนี้งานวิจัยของ Stavrou et al. (2020) ซึ่งได้ศึกษากระบวนการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ในระดับบัณฑิตศึกษาได้ให้ความสำคัญในเรื่องการวิจัยเชิงพัฒนาเพื่อเป็นการต่อยอดองค์ความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ในสายวิชาการ โดยหลักสูตรจะต้องเป็นแบบผสมผสานระหว่างการเรียนแบบตัวต่อตัวและแบบทางไกลไปสู่การทำวิจัยที่มีคุณภาพ งานวิจัยนี้สอดคล้องกับงานวิจัยของ Ahmed et al. (2020) ที่อธิบายถึงแนวคิดการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์ในระบบทางไกล ซึ่งผู้เรียนจะสามารถเรียนรู้ได้จากทั่วทุกหนทุกแห่งผ่านทางแพลตฟอร์มแบบออนไลน์ที่เตรียมขึ้น โดยรูปแบบของหลักสูตรออนไลน์นี้จะต้องมีการออกแบบให้เหมาะสมกับความต้องการของผู้เรียน โดยเน้นผู้เรียนให้มีส่วนร่วม และสนุกสนานไปกับกิจกรรมการเรียนการสอน และปรับเปลี่ยนเนื้อหาให้สอดคล้องตามภูมิหลังทางการศึกษาที่หลากหลายของผู้เรียน

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า งานวิจัยส่วนใหญ่เน้นการจัดรูปแบบหลักสูตรให้เหมาะสมกับผู้เรียน โดยมีการเรียนการสอนองค์ความรู้ขั้นพื้นฐาน ขั้นกลาง และขั้นสูง เพื่อให้ครอบคลุมองค์ความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ทุกประเด็น เน้นการฝึกปฏิบัติที่มีโจทย์จำลองเสมือนจริง โดยใช้แพลตฟอร์มออนไลน์เป็นสื่อกลางในการเรียนการสอน และเน้นการทำงานเป็นทีมควบคู่ไปกับหลักจรรยาบรรณทางวิชาชีพที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ระเบียบวิธีวิจัย

1) ประชากรและกลุ่มตัวอย่าง

(1) ประชากรของการศึกษาวิจัยในครั้งนี้ ได้แก่ นักเรียนนายร้อยตำรวจทั้ง 4 ชั้นปี ที่ศึกษาในโรงเรียนนายร้อยตำรวจระหว่างปีการศึกษา 2561 จนถึงปีการศึกษา 2564

(2) กลุ่มตัวอย่างของการศึกษาวิจัยในครั้งนี้ ได้แก่ นักเรียนนายร้อยตำรวจที่มีความรู้พื้นฐานและมีความสนใจทางด้านความมั่นคงปลอดภัยไซเบอร์จำนวน 40 คน ต่อปีการศึกษา โดยใช้การสุ่ม

ตัวอย่างแบบง่าย (Sample Random Sampling) เพื่อเลือกกลุ่มตัวอย่างในการเข้าร่วมฝึกอบรมในหลักสูตรทางด้านความมั่งคงปลอดภัยไซเบอร์ที่ได้ออกแบบขึ้น

2) ขั้นตอนการดำเนินกิจกรรมเพื่อให้ได้มาซึ่งแนวทางปฏิบัติที่ดี

การดำเนินกิจกรรมเพื่อออกแบบ ทดลอง และพัฒนาแนวทางปฏิบัติที่ดีสำหรับหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ของโรงเรียนนายร้อยตำรวจ ได้ใช้รูปแบบการลำดับขั้นตอนตามแบบพีดีซีเอ (PDCA: Plan–Do–Check–Act) ของ Deming (1986) และ Shewhart (1986) ซึ่งประกอบไปด้วย 4 ขั้นตอนดังต่อไปนี้

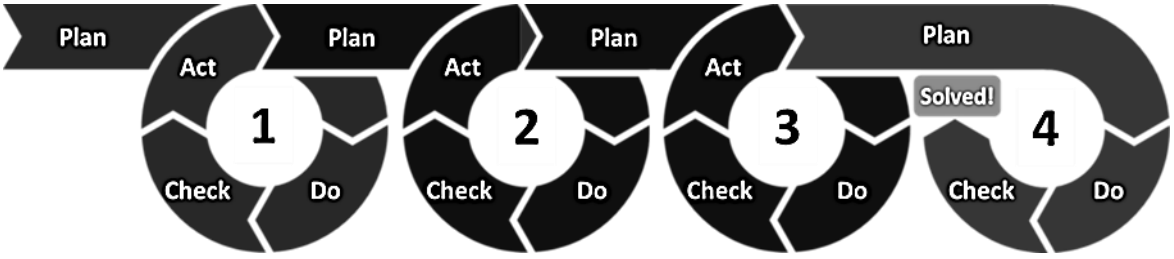
(1) การวางแผน (Plan) ซึ่งเป็นการวางแผนสำหรับการออกแบบเนื้อหาในหลักสูตรความมั่นคงปลอดภัยไซเบอร์ รวมถึงการกำหนดเนื้อหาและหัวข้อที่ต้องการปรับปรุงเปลี่ยนแปลง พร้อมทั้งการแก้ปัญหาที่เกิดขึ้นจากการเรียนการสอน

(2) การปฏิบัติตามแผน (Do) ซึ่งเป็นการดำเนินการจัดกิจกรรมในส่วนการเรียนการสอนตามหลักสูตรความมั่นคงปลอดภัยไซเบอร์ที่ได้ออกแบบขึ้น โดยมีโครงสร้าง การดำเนินการ และวิธีการดำเนินการตามแผนที่กำหนดไว้

(3) การตรวจสอบการปฏิบัติตามแผน (Check) ซึ่งเป็นการประเมินผลสัมฤทธิ์จากการดำเนินกิจกรรมการเรียนการสอนตามโครงสร้างหลักสูตรความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งมีการประเมินขั้นตอนการดำเนินงาน และการประเมินผลของการดำเนินงานตามแผนที่กำหนดไว้

(4) การปรับปรุงแก้ไข (Act) เป็นการนำผลการประเมินจากการจัดกิจกรรมทางการเรียนการสอนในหลักสูตรความมั่นคงปลอดภัยไซเบอร์มาวิเคราะห์ว่า มีโครงสร้างหรือขั้นตอนของการเรียนการสอนใดบ้างที่จะต้องปรับปรุงหรือพัฒนาให้ดีขึ้น

โดยกระบวนการตามแนวปฏิบัติที่ดีจากการศึกษาวิจัยในครั้งนี้ จะทำซ้ำตามแบบแผนพีดีซีเอจำนวน 4 วงรอบแบบคู่ขนาน ได้แก่ 1) วงรอบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ในระดับโรงเรียนทหาร-ตำรวจ 2) วงรอบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ในระดับชาติ 3) วงรอบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ในระดับนานาชาติ และ 4) วงรอบการสร้างนายตำรวจไซเบอร์เพื่อออกไปปฏิบัติหน้าที่ให้กับสำนักงานตำรวจแห่งชาติ ดังแสดงแผนผังการดำเนินงานตามภาพที่ 2



ภาพที่ 2 แบบแผนพีดีซีเอจำนวน 4 วงรอบแบบคู่ขนาน

3) เครื่องมือการวิจัย

การศึกษาวิจัยในครั้งนี้ใช้กระบวนการทดลองโดยการนำนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมาร่วมทำกิจกรรมการเรียนการสอนตามหลักสูตรความมั่นคงปลอดภัยไซเบอร์ที่ได้ออกแบบขึ้นเป็น

ระยะเวลา 2 เดือน หลังจากนั้นจะใช้แบบทดสอบในการประเมินผลเชิงปริมาณ ซึ่งพิจารณาจากความรู้ความเข้าใจของนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างที่ได้รับระหว่างการเข้าร่วมกิจกรรม พร้อมทั้งใช้แบบสังเกตการณ์ในการวัดผลเชิงคุณภาพ โดยดูจากพฤติกรรมความกระตือรือร้นและความสนใจในการเข้าร่วมกิจกรรมการเรียนการสอน นอกจากนี้ยังใช้เครื่องมือที่เป็นการแข่งขันทักษะทางไซเบอร์ทั้งในระดับเหล่าทัพ ระดับชาติ และระดับนานาชาติ เป็นตัวชี้วัดถึงความสำเร็จของการเรียนการสอนตามหลักสูตรความมั่นคงปลอดภัยไซเบอร์ที่ได้ออกแบบขึ้นอีกด้วย

ผลการวิจัย

ผลลัพธ์การวิจัยจากการใช้แบบแผนพีดีซีเอจำนวน 4 วงรอบแบบคู่ขนานมีรายละเอียดดังต่อไปนี้

1) ผลลัพธ์จากวงรอบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ในระดับโรงเรียนทหาร-ตำรวจ

ขั้นตอนที่ 1 การวางแผนการดำเนินกิจกรรม : วางแผน (Plan) ซึ่งประกอบไปด้วย

(1) การกำหนดวิธีการคัดเลือกนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างที่จะเข้าร่วมกิจกรรมการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ โดยใช้การจัดอันดับผลการทดสอบและการสัมภาษณ์ ซึ่งนักเรียนนายร้อยตำรวจที่ได้รับการคัดเลือกจะต้องมีความรู้พื้นฐานทางด้านคอมพิวเตอร์ เช่น การเขียนโปรแกรมคอมพิวเตอร์เบื้องต้น การเขียนเว็บเบื้องต้น และการใช้คำสั่งการเชื่อมต่อระบบเครือข่าย เป็นต้น

(2) กำหนดโครงสร้างของหลักสูตรการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์โดยแบ่งออกเป็น 2 ส่วน ได้แก่ การศึกษาความรู้พื้นฐานด้านวิทยาการคอมพิวเตอร์ที่จำเป็นสำหรับการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดของเนื้อหาตามตารางที่ 1 และ การศึกษาความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์ที่ประกอบไปด้วยความมั่นคงปลอดภัยไซเบอร์เชิงรุก (Offensive Cybersecurity) โดยมีรายละเอียดของเนื้อหาตามตารางที่ 2 และความมั่นคงปลอดภัยไซเบอร์เชิงรับ (Defensive Cybersecurity) โดยมีรายละเอียดของเนื้อหาตามตารางที่ 3

ตารางที่ 1 รายละเอียดของเนื้อหาสำหรับการศึกษาความรู้พื้นฐานด้านวิทยาการคอมพิวเตอร์ที่จำเป็นสำหรับการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	เนื้อหา	จำนวนชั่วโมง
1.	เครื่องมือทางด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Tools)	3
2.	การเขียนโปรแกรมคอมพิวเตอร์ (Computer Programming)	6
3.	ระบบปฏิบัติการยูนิกส์ (Unix Operating System)	3
4.	ระบบปฏิบัติการเอ็มเอสดอส (MS-DOS Operating System)	3
5.	เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต (Computer Network and Internet)	6
6.	ระบบและโครงสร้างของเว็บ (Web Systems and Structures)	6
7.	ระบบแฟ้มข้อมูลและฐานข้อมูล (File and Database System)	3
	รวมทั้งสิ้น	**30**

ตารางที่ 2 รายละเอียดของเนื้อหาสำหรับการศึกษาความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์เชิงรุก

ลำดับ	เนื้อหา	จำนวนชั่วโมง
1.	การเขียนโปรแกรมสำหรับการแฮ็กอย่างมีจรรยาบรรณ (Programming for Ethical Hacking)	12
2.	การเข้าถึงทรัพยากรของเครือข่าย (Network Exploitations)	9
3.	การเข้าถึงทรัพยากรของเครื่อง (Machine Exploitations)	9
4.	การเข้าถึงทรัพยากรของเว็บ (Web Exploitations)	12
5.	การยึดครอง (Pwnable)	9
	รวมทั้งสิ้น	**51**

ตารางที่ 3 รายละเอียดของเนื้อหาสำหรับการศึกษาความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์เชิงรับ

ลำดับ	เนื้อหา	จำนวนชั่วโมง
1.	การทำวิศวกรรมย้อนกลับ (Reverse Engineering)	9
2.	การตรวจพิสูจน์ทางดิจิทัล (Digital Forensics)	9
3.	วิทยาการเข้ารหัสลับ (Cryptography)	9
4.	การใช้เครื่องมือโอเอสไอเอ็นที (OSINT: Open-Source Intelligence)	9
5.	ความรู้เบ็ดเตล็ต (Miscellaneous)	6
	รวมทั้งสิ้น	**42**

(3) กำหนดรูปแบบการสอนด้านความมั่นคงปลอดภัยไซเบอร์โดยใช้การเรียนรู้ด้วยเกม (Game Based Learning: GBL) ซึ่งเกมที่นำมาใช้ในการสอนด้านความมั่นคงปลอดภัยไซเบอร์ในครั้งนี้คือ เกมซีทีเอฟหรือเกมยึดธง (Capture The Flag: CTF) ซึ่งธงจะอยู่ในรูปแบบของรหัสหรือข้อความเฉพาะที่สามารถสังเกตได้ โดยเกมยึดธงนี้เป็นที่นิยมในการวงการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก

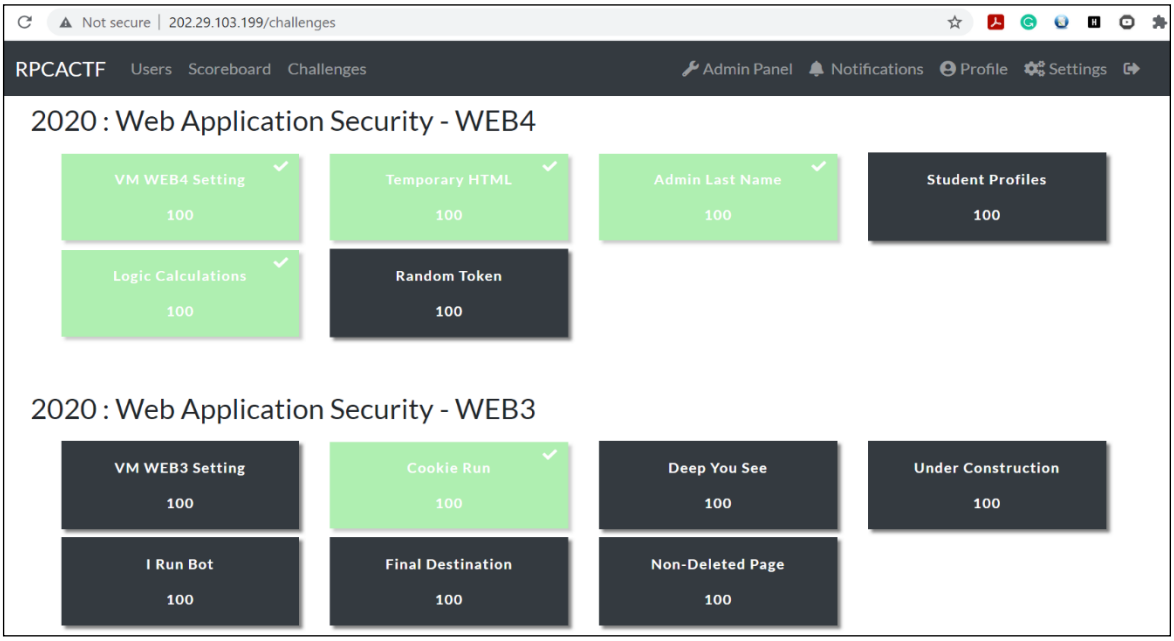
(4) กำหนดการฝึกปฏิบัติและการทำกิจกรรมในการเรียนการสอนโดยใช้ระบบ CTFd (2021) ซึ่งเป็นเครื่องมือแบบฟรีแวร์ (Freeware) ที่พัฒนาบนระบบเว็บ และเปิดให้บุคคลทั่วไปนำไปใช้ในการเรียนการสอนและจัดการแข่งขันทางด้านความมั่นคงปลอดภัยไซเบอร์โดยมีรายละเอียดตามภาพที่ 3

(5) กำหนดการวัดผลการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์โดยใช้การทดสอบในการวัดผลเชิงปริมาณ ซึ่งผู้เรียนจะต้องมีคะแนนวัดผลความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่าร้อยละ 60 และใช้การสังเกตในการวัดผลเชิงคุณภาพ ซึ่งเป็นการศึกษาถึงพฤติกรรมของผู้เรียนในการเลือกใช้เทคนิคและองค์ความรู้ที่นำไปใช้ในการแก้ปัญหาตามโจทย์หรือภารกิจที่ได้รับมอบหมาย และการศึกษาไทม์ไลน์ของผู้เรียนที่ใช้ความพยายามในการทำโจทย์ให้ได้คำตอบที่ถูกต้อง และเป็นไปตามแนวทางที่กำหนดไว้

ภาพที่ 3 ระบบ CTFd สำหรับการเรียนการสอนและการฝึกปฏิบัติทางด้านความมั่นคงปลอดภัยไซเบอร์

ขั้นตอนที่ 2 การดำเนินกิจกรรมตามแผน : ปฏิบัติตามแผน (Do)

ดำเนินกิจกรรมการเรียนการสอนตามแผนที่กำหนดไว้ โดยใช้ระบบปฏิบัติการแคลิลีนุกซ์ (Kali Linux) เป็นเครื่องมือหลักในการเรียนการสอน ซึ่งภายในแคลิลีนุกซ์นี้จะมีทั้งเครื่องมือความปลอดภัยไซเบอร์เชิงรุกและเชิงรับ โดยให้นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างทำการฝึกปฏิบัติและฝึกทำภารกิจทางด้านความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบ CTFd เพื่อค้นหาและยึดธงตามรูปแบบของเกมซีทีเอฟ ซึ่งมีตัวอย่างตามภาพที่ 4



ภาพที่ 4 การฝึกปฏิบัติและฝึกทำภารกิจทางด้านความมั่นคงปลอดภัยไซเบอร์โดยใช้ระบบ CTFd

ขั้นตอนที่ 3 การติดตามตรวจสอบประเมินผลกิจกรรม : ตรวจสอบการปฏิบัติตามแผน (Check)

การดำเนินการประเมินผลการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ ได้ใช้การทดสอบในการวัดผลเชิงปริมาณ ซึ่งผู้เรียนจะต้องมีคะแนนวัดผลความรู้ความเข้าใจด้าน ความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่าร้อยละ 60 โดยมีผลคะแนนการทดสอบดังตารางที่ 4

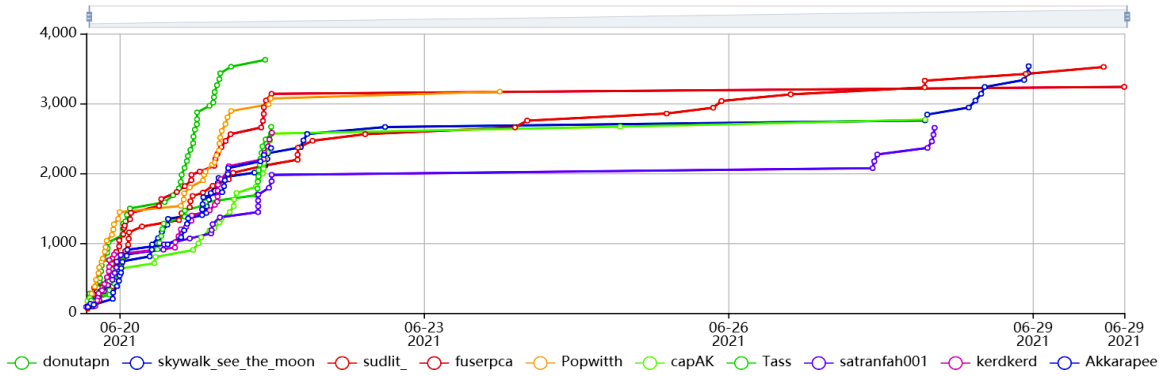
ตารางที่ 4 ผลคะแนนการประเมินการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์โดยใช้การทดสอบ

นรต. กลุ่มตัวอย่าง	คะแนนพื้นฐานทางวิทยาการคอมพิวเตอร์ (ร้อยละ)	คะแนนความมั่นคงปลอดภัยไซเบอร์เชิงรุก (ร้อยละ)	คะแนนความมั่นคงปลอดภัยไซเบอร์เชิงรับ (ร้อยละ)
คนที่ 1	78	78	90
คนที่ 2	77	71	78
คนที่ 3	87	77	81
คนที่ 4	94	86	80
คนที่ 5	94	74	88
คนที่ 6	78	66	82
คนที่ 7	91	89	96
คนที่ 8	88	65	76
คนที่ 9	86	72	78
คนที่ 10	75	79	89
คนที่ 11	83	81	81
คนที่ 12	82	71	86
คนที่ 13	96	84	85
คนที่ 14	88	84	76
คนที่ 15	84	91	96
คนที่ 16	77	86	72
คนที่ 17	91	71	70
คนที่ 18	94	86	89
คนที่ 19	90	82	82
คนที่ 20	91	86	76
คนที่ 21	87	76	82
คนที่ 22	87	67	86
คนที่ 23	93	71	94
คนที่ 24	89	71	71
คนที่ 25	77	87	92

นรต. กลุ่มตัวอย่าง	คะแนนพื้นฐานทางวิทยาการคอมพิวเตอร์ (ร้อยละ)	คะแนนความมั่นคงปลอดภัยไซเบอร์เชิงรุก (ร้อยละ)	คะแนนความมั่นคงปลอดภัยไซเบอร์เชิงรับ (ร้อยละ)
คนที่ 26	90	86	80
คนที่ 27	92	71	76
คนที่ 28	77	84	71
คนที่ 29	75	72	71
คนที่ 30	92	89	79
คนที่ 31	76	75	77
คนที่ 32	91	90	82
คนที่ 33	85	68	92
คนที่ 34	79	91	90
คนที่ 35	85	67	72
คนที่ 36	77	71	81
คนที่ 37	85	75	89
คนที่ 38	91	79	89
คนที่ 39	96	91	83
คนที่ 40	80	75	79
เฉลี่ย	**85.70**	**78.38**	**82.18**

จากผลลัพธ์ในตารางที่ 4 แสดงให้เห็นว่านักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมีผลคะแนนเกินกว่าร้อยละ 60 ทุกคน คิดเป็นร้อยละ 100 ของจำนวนผู้ที่ผ่านการประเมิน โดยนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างที่มีความถนัดในด้านความมั่นคงปลอดภัยไซเบอร์เชิงรุกจำนวน 12 คน มีความถนัดในด้านความมั่นคงปลอดภัยไซเบอร์เชิงรับจำนวน 25 คน และมีความถนัดทั้งสองด้านจำนวน 3 คน โดยเนื้อหาที่นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมีความถนัดมากที่สุดคือเนื้อหาเรื่องการตรวจพิสูจน์ทางดิจิทัล (Digital Forensic) และวิทยาการเข้ารหัสลับ (Cryptography)

การดำเนินการประเมินผลการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์โดยใช้การสังเกตในการวัดผลเชิงคุณภาพ ซึ่งเป็นการศึกษาถึงพฤติกรรมของผู้เรียนในการเลือกใช้เทคนิคและองค์ความรู้ที่นำไปใช้ในการแก้ปัญหาตามโจทย์หรือภารกิจที่ได้รับมอบหมาย และการศึกษาไทม์ไลน์ของผู้เรียนที่ใช้ความพยายามในการทำโจทย์ให้ได้มาซึ่งคำตอบที่ถูกต้อง โดยมีผลการวิเคราะห์ตามกราฟในภาพที่ 5 โดยจากผลการศึกษาพฤติกรรมของนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างในการเลือกใช้เทคนิคและองค์ความรู้ที่นำไปใช้ในการแก้ปัญหาตามโจทย์หรือภารกิจที่ได้รับมอบหมายพบว่า ผู้เรียนมีการใช้เทคนิคที่หลากหลายตามความถนัดของตัวเอง บางเทคนิคก็เป็นวิธีแปลกใหม่ที่ผู้วิจัยไม่คิดว่านักเรียนนายร้อยตำรวจกลุ่มตัวอย่างจะเลือกใช้วิธีดังกล่าวในการแก้ปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์ ในขณะที่การศึกษาไทม์ไลน์ของผู้เรียนที่ใช้ความพยายามในการทำโจทย์ให้ได้คำตอบที่ถูกต้อง พบว่าผู้เรียนมักจะคาดเดาคำตอบโดยการสุ่มตอบ และทดลองป้อนคำตอบจนกว่าจะได้คำตอบที่ถูกต้อง



ภาพที่ 5 การศึกษาไทม์ไลน์จากความพยายามในการทำโจทย์เพื่อให้ได้มาซึ่งคำตอบที่ถูกต้อง

ผลลัพธ์จากการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ในวงรอบนี้ นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างได้เข้าร่วมการแข่งขันทักษะทางไซเบอร์ระดับโรงเรียนทหาร-ตำรวจ ตั้งแต่ปี 2561 ถึงปี 2564 โดยการแข่งขันประจำปี 2561 ได้รับรางวัลรองชนะเลิศอันดับ 1 การแข่งขันประจำปี 2562 ได้รับรางวัลรองชนะเลิศอันดับ 1 การแข่งขันทักษะทางไซเบอร์ประจำปี 2563 ได้รับรางวัลชนะเลิศ และ การแข่งขันทักษะทางไซเบอร์ประจำปี 2564 ได้รับรางวัลชนะเลิศ

ขั้นตอนที่ 4 การปรับปรุงแก้ไขแผนกิจกรรม : ปรับปรุงแก้ไข (Act)

เป็นการนำคำแนะนำจากนักเรียนนายร้อยตำรวจกลุ่มตัวอย่าง มาปรับปรุงและแก้ไข โดยตรวจสอบกิจกรรมที่ควรปรับปรุงและพัฒนาให้เหมาะสมและดียิ่งขึ้น โดยนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างต้องการให้จัดระดับของโจทย์และภารกิจจากระดับง่ายไปจนถึงระดับยาก ต้องการเวลาในการศึกษาหาความรู้เพิ่มเติมในเนื้อหาหมวดต่าง ๆ ต้องการเวลาในการฝึกปฏิบัติตามโจทย์ฝึกให้มากยิ่งขึ้น และต้องการให้อาจารย์ผู้สอน (ผู้วิจัย) มีการปรับปรุงหลักสูตรรัฐประศาสนศาสตรบัณฑิตของโรงเรียนนายร้อยตำรวจ ให้สอดแทรกกิจกรรมตามหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์นี้

2) ผลลัพธ์จากวงรอบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ในระดับชาติ

(1) ขั้นตอนที่ 1 การวางแผนการดำเนินกิจกรรม : วางแผน (Plan) ได้ใช้แผนการดำเนินกิจกรรมตามวงรอบที่ 1 โดยมีการปรับปรุงในส่วนของการกำหนดโจทย์ฝึกและแบบทดสอบให้ตรงตามสถานการณ์จริงที่เกิดขึ้นในวงการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

(2) ขั้นตอนที่ 2 การดำเนินกิจกรรมตามแผน : ปฏิบัติตามแผน (Do) การดำเนินการกิจกรรมได้ทำตามวงรอบที่ 1 แต่มีการเจาะลึกในเนื้อหาของแต่ละหมวดมากยิ่งขึ้น มีการกำหนดภารกิจของโจทย์ฝึกปฏิบัติที่สมจริงมากยิ่งขึ้น

(3) ขั้นตอนที่ 3 การติดตามตรวจสอบประเมินผลกิจกรรม : ตรวจสอบการปฏิบัติตามแผน (Check) ผลการดำเนินการพบว่านักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมีทักษะทางด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มมากยิ่งขึ้น โดยสามารถทำคะแนนการทดสอบได้เกินกว่าร้อยละ 80 เป็นจำนวนเพิ่มขึ้นจากวงรอบที่ 1 นอกจากนี้ผลการสอนด้านความมั่นคงปลอดภัยไซเบอร์ในวงรอบนี้ ทำให้นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างมีโอกาสได้เข้าร่วมการแข่งขันทักษะทางไซเบอร์ในระดับชาติและทำผลงานได้เป็นที่ประจักษ์ดังนี้ การแข่งขัน TCSD Cyber Competition 2019 ได้รับรางวัลชนะเลิศ การแข่งขัน

STDiO CTF Competition 2020 ได้รับรางวัลชนะเลิศ การแข่งขัน Thailand Cyber Top Students 2021 ได้รับรางวัลชนะเลิศ การแข่งขัน Palo Alto Networks Capture the Flag Capture the Future Competition 2021 ได้รับรางวัลรองชนะเลิศอันดับ 1 และ การแข่งขัน KPMG Cyber Security Challenge 2021 ได้รับรางวัลรองชนะเลิศอันดับ 1

(4) ขั้นตอนที่ 4 การปรับปรุงแก้ไขแผนกิจกรรม : ปรับปรุงแก้ไข (Act) นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างต้องการให้เพิ่มความหลากหลายของโจทย์ฝึกที่เป็นมาตรฐานตามแบบสากล

3) ผลลัพธ์จากวงรอบการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ประจักษ์ในระดับนานาชาติ

(1) ขั้นตอนที่ 1 การวางแผนการดำเนินกิจกรรม : วางแผน (Plan) ได้ใช้แผนการดำเนินกิจกรรมตามวงรอบที่ 1 และวงรอบที่ 2 โดยมีการปรับปรุงในส่วนของการกำหนดโจทย์ฝึกและแบบทดสอบให้ตรงตามสถานการณ์จริงที่เกิดขึ้นในวงการไซเบอร์ทั่วโลก เพื่อต้องการให้นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างได้เห็นรูปแบบของภัยคุกคามทางไซเบอร์ทั่วทุกมุมโลก และเพื่อให้นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างได้ศึกษาถึงเทคนิคที่จะนำมาใช้ในการแก้ปัญหาเหล่านั้น

(2) ขั้นตอนที่ 2 การดำเนินกิจกรรมตามแผน : ปฏิบัติตามแผน (Do) การดำเนินการกิจกรรมได้ทำตามวงรอบที่ 1 และวงรอบที่ 2 โดยเพิ่มความเข้มข้นในเนื้อหาที่ใช้ในการเรียนการสอน มีการแสดงรายละเอียดของเทคนิคในการแก้ปัญหาทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ซับซ้อนขึ้น และมีการนำเอาองค์ความรู้ที่เผยแพร่ในระดับสากลมาใช้ในกิจกรรมการเรียนการสอน

(3) ขั้นตอนที่ 3 การติดตามตรวจสอบประเมินผลกิจกรรม : ตรวจสอบการปฏิบัติตามแผน (Check) นักเรียนนายร้อยตำรวจกลุ่มตัวอย่างได้เข้าร่วมการแข่งขันทักษะทางไซเบอร์ในระดับนานาชาติรายการ BSides Delhi CTF 2020 ซึ่งเป็นการแข่งขันทักษะทางไซเบอร์ระดับนานาชาติแบบออนไลน์ของประเทศอินเดีย โดยทำผลงานเป็นอันดับที่ 7 ของโลก (เป็นอันดับที่ 1 ของตัวแทนประเทศไทย จากทีมเข้าร่วมการแข่งขัน 130 ทีมทั่วโลก) การแข่งขันรายการ HACON CTF 2020 ของประเทศสหรัฐอาหรับเอมิเรตส์ โดยทำผลงานเป็นอันดับที่ 13 ของโลก (เป็นอันดับที่ 1 ของตัวแทนประเทศไทย จากทีมเข้าร่วมการแข่งขัน 209 ทีมทั่วโลก) และ การแข่งขันรายการ UMDCTF 2021 ของประเทศสหรัฐอเมริกา โดยทำผลงานเป็นอันดับที่ 9 ของโลก (เป็นอันดับที่ 1 ของตัวแทนประเทศไทย จากทีมเข้าร่วมการแข่งขัน 484 ทีมทั่วโลก)

(4) ขั้นตอนที่ 4 การปรับปรุงแก้ไขแผนกิจกรรม : ปรับปรุงแก้ไข (Act) โดยการปรับปรุงได้กำหนดให้เป็นไปตามวงรอบที่ 1 และวงรอบที่ 2

4) วงรอบการสร้างนายตำรวจไซเบอร์เพื่อออกไปปฏิบัติหน้าที่ให้กับสำนักงานตำรวจแห่งชาติ

(1) ขั้นตอนที่ 1 การวางแผนการดำเนินกิจกรรม : วางแผน (Plan) ได้วางแผนในการส่งรายชื่อว่าที่นายตำรวจไซเบอร์ที่กำลังจะสำเร็จการศึกษาในแต่ละปีการศึกษาให้กับกองบัญชาการต่าง ๆ ภายใต้สังกัดสำนักงานตำรวจแห่งชาติที่มีความต้องการนายตำรวจทางด้านความมั่นคงปลอดภัยไซเบอร์ เช่น กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี และ สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร เป็นต้น

(2) ขั้นตอนที่ 2 การดำเนินกิจกรรมตามแผน : ปฏิบัติตามแผน (Do) ได้คัดเลือกว่าที่นายตำรวจไซเบอร์ในแต่ละปีการศึกษาจำนวน 4-8 นาย เพื่อส่งต่อให้หน่วยงานของสำนักงานตำรวจแห่งชาติ ตามแผนการคัดเลือกที่กำหนดไว้ในขั้นตอนที่ 1

(3) ขั้นตอนที่ 3 การติดตามตรวจสอบประเมินผลกิจกรรม : ตรวจสอบการปฏิบัติตามแผน (Check) นายตำรวจไซเบอร์ที่ไปปฏิบัติงานตามหน่วยงานต่าง ๆ ของสำนักงานตำรวจแห่งชาติ ได้รับการชื่นชมจากผู้บังคับบัญชาและผู้ใช้บัณฑิต โดยผู้บังคับบัญชามีความประสงค์ในการคัดเลือกตัวว่าที่นายตำรวจไซเบอร์ให้ไปปฏิบัติหน้าที่พิเศษที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เช่น การสืบสวนทางไซเบอร์ขั้นสูง และการตรวจพิสูจน์ทางดิจิทัลขั้นสูง เป็นต้น

(4) ขั้นตอนที่ 4 การปรับปรุงแก้ไขแผนกิจกรรม : ปรับปรุงแก้ไข (Act) ปรับปรุงกระบวนการเลือกตำแหน่งของนักเรียนนายร้อยตำรวจกลุ่มตัวอย่างที่จบใหม่ให้มีความเฉพาะเจาะจงในตำแหน่งทางด้านความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น

สรุปและอภิปรายผล

การศึกษาวิจัยเรื่องนี้ทำให้ได้แนวปฏิบัติที่ดีที่เป็นหลักสูตรต้นแบบของการเรียนการสอนทางด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโรงเรียนนายร้อยตำรวจ โดยโครงสร้างของหลักสูตรแบ่งออกเป็น 2 ส่วน ได้แก่ 1) การศึกษาความรู้พื้นฐานด้านวิทยาการคอมพิวเตอร์ที่จำเป็นสำหรับการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และ 2) การศึกษาความรู้หลักด้านความมั่นคงปลอดภัยไซเบอร์เชิงรุกและเชิงรับ โดยจัดกิจกรรมการเรียนการสอนในรูปแบบเกมซีทีเอฟบนระบบออนไลน์ การศึกษาวิจัยเรื่องนี้ใช้แบบแผนพีดีซีเอจำนวน 4 วงรอบแบบคู่ขนาน ในการกำหนดขั้นตอนการดำเนินงานของแนวปฏิบัติที่ดี ซึ่งหลักสูตรต้นแบบนี้ก่อให้เกิดการส่งเสริมและการพัฒนาเนื้อหาในรายวิชาความมั่นคงปลอดภัยไซเบอร์ของโรงเรียนนายร้อยตำรวจให้ได้มาตรฐานและมีประสิทธิภาพในระดับสากล ทั้งยังสามารถผลิตนายตำรวจยุคใหม่ที่มีทักษะและองค์ความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ครบถ้วนสมบูรณ์ และมีผลสัมฤทธิ์ที่เป็นที่ประจักษ์ในระดับเหล่าทัพ ระดับชาติ และระดับนานาชาติ

เอกสารอ้างอิง

Ahmed, A., Lundqvist, K., Watterson, C., and Baghaei, N. (2020). **Teaching cybersecurity for distance learners: A reflective study**. In Proceedings of Frontiers in Education Conference, FIE, 2020-October.

Chulalongkorn University. (2018). **Bachelor of Engineering Program in Computer Engineering 2018 Revision**, Academic Document of the Department of Computer Engineering, Faculty of Engineering, Retrieved from https://www.cp.eng.chula.ac.th/future/bachelor. (In Thai).

Crick, T., Davenport, J. H., Irons, A., and Prickett, T. (2019). **A UK case study on cyber security education and accreditation**. In Proceedings of Frontiers in Education Conference, FIE, 2019-October.

CTFd. (2021). **Cybersecurity Training Platform with Capture The Flag**. Retrieved May 29, 2021, from https://ctfd.io/.

Dai, J. (2019). **Situation awareness-oriented cybersecurity education**. In Proceedings of Frontiers in Education Conference, FIE, 2018-October.

Deming, W. E. (1986). **Out of the crisis**. Cambridge, MA: Massachusetts Institute of Technology, Center for Advanced Engineering Study. p. 88.

King Mongkut's University of Technology Thonburi. (2017). **Bachelor of Science Program in Applied Computer Science 2017 Revision**, Academic Document of the Department of Mathematics, Faculty of Science, King Mongkut's University of Technology Thonburi, Retrieved from https://math.kmutt.ac.th/index.php/academic-admission/undergraduate/b-sc-applied-computer-science. (In Thai).

Mahidol University. (2018). **Bachelor of Science in Information and Communication Technology (International Program) 2018 Revision**, Academic Document of the Faculty of Information and Communication Technology, Mahidol University, Retrieved from https://www.ict.mahidol.ac.th/th/?page_id=679. (In Thai).

Omar, T., Venkatesan, S., and Amamra, A. (2018). **Development of undergraduate interdisciplinary cybersecurity program: A literature survey**. In Proceedings of ASEE Annual Conference and Exposition, Conference, 2018-June.

Peruma, A., Malachowsky, S. A., and Krutz, D. E. (2018). **Providing an experiential cyber security learning experience through mobile security labs.** In Proceedings of International Conference on Software Engineering, 51-54.

Royal Police Cadet Academy. (2018). **Bachelor of Public Administration Program in Police Science 2018 Revision**, Academic Book of Royal Police Cadet Academy. (In Thai).

Shewhart, W. A. (1986). **Statistical method from the viewpoint of quality control**. New York: Dover.

Stavrou, E., and Polycarpou, I. (2020). **Cybersecurity-related curriculum for diverse postgraduate cohorts: A case study**. In Proceedings of 14th International Multi-Conference on Society, Cybernetics and Informatics, 88-93.

Yuan, X., Zhang, T., Shama, A. A., Xu, J., Yang, L., Ellis, J., and Waters, C. (2019). **Teaching cybersecurity using guided inquiry collaborative learning**. In Proceedings of Frontiers in Education Conference, FIE, 2019-October.

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล **พันตำรวจตรี ดร.วงศ์ยศ เกิดศรี ***
ตำแหน่ง/สถานะ อาจารย์ (สัญญาบัตร 2)
ที่อยู่หน่วยงาน/สังกัด คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110
ไปรษณีย์อิเล็กทรอนิกส์ wongyos@gmail.com, wongyos@rpca.ac.th

* ผู้ประพันธ์บรรณกิจ (Corresponding Author)