รายละเอียดของรายวิชา

ชื่อสถาบันอุดมศึกษา มหาวิทยาลัยราชภัฏอุบลราชธานี

วิทยาเขต/คณะ/ภาควิชา คณะเทคโนโลยีอุตสาหกรรม สาขาวิชาวิศวกรรมเครือข่ายคอมพิวเตอร์

หมวดที่ 1 ลักษณะและข้อมูลโดยทั่วไปของรายวิชา

1. รหัสและชื่อรายวิชา

7024713 อาชญากรรมไซเบอร์และการพิสูจน์หลักฐานดิจิทัล

Cyber Crime and Digital Forensics

2. จำนวนหน่วยกิต

3 หน่วยกิต (2 – 2 – 5)

3. หลักสูตรและประเภทรายวิชา

วิศวกรรมศาสตรบัณฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์ รายวิชาชีพ (บังคับ)

4. อาจารย์ผู้รับผิดชอบรายวิชา

รองศาสตราจารย์เอกรินทร์ วทัญญูเลิศสกุล อาจารย์ผู้สอน

5. ภาคการศึกษา / ชั้นปีที่เรียน

ภาคการศึกษาที่ 1 / 2567 ชั้นปีที่ 4 กลุ่มที่ 1

6. รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite) (ถ้ามี)

ไม่มี

7. รายวิชาที่ต้องเรียนพร้อมกัน (Co-requisites) (ถ้ามี)

ไม่มี

8. สถานที่เรียน

คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏอุบลราชธานี

9. วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด

15 มิถุนายน 2567

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

1. จุดมุ่งหมายของรายวิชา

1. นักศึกษามีความรู้ความเข้าใจพื้นฐานเกี่ยวกับความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

2. นักศึกษามีความรู้ความเข้าใจเกี่ยวกับนโยบายและมาตรฐานความมั่นคงปลอดภัย

3. นักศึกษามีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามในรูปแบบต่างๆ และการป้องกันการเจาะระบบเครือข่ายคอมพิวเตอร์

4. นักศึกษามีความรู้ความเข้าใจหลักการควบคุมการเข้าถึงความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

2. วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา

เพื่อพัฒนาการเรียนการสอนที่เสริมสร้างความรู้ความเข้าใจเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กฎหมายที่เกี่ยวข้อง และรูปแบบของอาชญากรรมไซเบอร์ พร้อมทั้งเสริมทักษะในการสืบสวนและพิสูจน์หลักฐานดิจิทัลอย่างเป็นระบบ โดยเน้นการเก็บรวบรวม วิเคราะห์ และประเมินหลักฐานจากระบบคอมพิวเตอร์และเครือข่าย ตลอดจนการประยุกต์ใช้กรณีศึกษาเพื่อเพิ่มความเข้าใจในสถานการณ์จริง อันเป็นการเตรียมความพร้อมให้ผู้เรียนสามารถประยุกต์ใช้ความรู้ในการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์และการพิสูจน์หลักฐานดิจิทัลในวิชาชีพได้อย่างมีประสิทธิภาพ

หมวดที่ 3 ส่วนประกอบของรายวิชา

1. คำอธิบายรายวิชา

แนะนำหลักการเบื้องต้นของอาชญากรรมทางคอมพิวเตอร์ กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ ลักษณะและชนิดของอาชญากรรมไซเบอร์ ขั้นตอนการสืบสวนอาชญากรรมทางคอมพิวเตอร์ การเก็บรวบรวมหลักฐานและการพิสูจน์หลักฐานดิจิทัลจากที่เกิดเหตุ ระบบไฟล์ข้อมูลของระบบปฏิบัติการต่าง ๆ การวิเคราะห์หลักฐานจากระบบปฏิบัติการ การเก็บหลักฐานดิจิทัลและการวิเคราะห์หลักฐานจากระบบเครือข่าย การวิเคราะห์หลักฐานการโจมตีระบบเครือข่าย กรณีศึกษาของการสืบสวนอาชญากรรมทางคอมพิวเตอร์

2. จำนวนชั่วโมงที่ใช้ต่อภาคการศึกษา

จำนวนชั่วโมงบรรยายต่อสัปดาห์	2	ชั่วโมง
จำนวนชั่วโมงฝึกปฏิบัติการต่อสัปดาห์	2	ชั่วโมง
จำนวนชั่วโมงการศึกษาด้วยตนเอง	5	ชั่วโมง
จำนวนชั่วโมงที่สอนเสริมในรายวิชา	สอนเสริมตามความต้องการของนักศึกษาเป็นกลุ่มและเฉพาะราย	

3. จำนวนชั่วโมงต่อสัปดาห์ที่อาจารย์ให้คำปรึกษาและแนะนำทางวิชาการแก่นักศึกษาเป็นรายบุคคล

อาจารย์จัดเวลาให้คำปรึกษาเป็นรายบุคคล หรือ รายกลุ่มตามความต้องการอย่างน้อย 1 ชั่วโมงต่อสัปดาห์ (เฉพาะรายที่ต้องการ) โดยการประกาศเวลาให้คำปรึกษาผ่านเว็บไซต์ของทางกลุ่มวิชา ฯ หรือตามตารางเวลาเข้าพบที่กำหนด

หมวดที่ 4 การพัฒนาการเรียนรู้ของนักศึกษา

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	วิธีการสอนที่จะใช้พัฒนาการเรียนรู้	วิธีการวัดและประเมินผล
1. คุณธรรม จริยธรรม - มีวินัย ตรงต่อเวลา และความรับผิดชอบต่อตนเอง วิชาชีพและสังคม - มีภาวะความเป็นผู้นำและผู้ตาม สามารถทำงานเป็นทีมและสามารถแก้ไขข้อขัดแย้งและลำดับความสำคัญ - เคารพสิทธิและรับฟังความคิดเห็นของผู้อื่น รวมทั้งเคารพในคุณค่าและศักดิ์ศรีของความเป็นมนุษย์ - มีจรรยาบรรณทางวิชาการและวิชาชีพ	- บรรยายถึงความจำเป็นของการมีวินัยและการมีความรับผิดชอบ ร่วมทั้งจัดให้มีการส่งงานและการตรวจสอบเวลาเข้าชั้นเรียนของนักศึกษา - จัดให้มีการอภิปรายกลุ่มหรือกำหนดให้นักศึกษาจัดทำโครงงานย่อยพร้อมจัดทำรายงานประกอบ - จัดให้มีการอภิปรายกลุ่มหรือกำหนดให้นักศึกษาจัดทำรายงานกลุ่มย่อยพร้อมจัดทำรายงานประกอบ	- พฤติกรรมนักศึกษาในการเข้าชั้นเรียน การส่งงานตามกำหนดระยะเวลาที่มอบหมายและการร่วมกิจกรรม - ประเมินจากการมีวินัยและพร้อมเพรียงของนักศึกษาในการเข้าร่วมกิจกรรมเสริมหลักสูตร - ประเมินจากการจัดทำรายงานและตรวจสอบความมีประสิทธิภาพการวางแผนในการดำเนินจัดทำรายงานกลุ่มและการปฏิบัติตามแผนของผู้ร่วมงาน - ประเมินจากความรับผิดชอบในหน้าที่ที่ได้รับมอบหมาย
2. ความรู้ - มีความรู้และความเข้าใจเกี่ยวกับหลักการและทฤษฎีที่สำคัญในเนื้อหาการรักษาความมั่นคงและบริหารความเสี่ยงระบบสารสนเทศ - สามารถวิเคราะห์ปัญหา เข้าใจและอธิบายความต้องการทางการรักษาความมั่นคงและบริหารความเสี่ยงระบบสารสนเทศรวมทั้งประยุกต์ความรู้ทักษะ และการใช้เครื่องมือที่เหมาะสมกับการแก้ไขปัญหา	- บรรยาย ฝึกปฏิบัติในห้องปฏิบัติการ - การทำงานกลุ่ม การนำเสนอผลการดำเนินการวิเคราะห์กรณีศึกษา - มอบหมายให้ค้นคว้าหาบทความ ข้อมูลที่เกี่ยวข้อง โดยนำมาสรุปและนำเสนอการศึกษาโดยใช้ปัญหา และโครงงานย่อย	- ทดสอบย่อย สอบกลางภาค สอบปลายภาค ด้วยข้อสอบอัตนัยและปรนัย - นำเสนอสรุปการอ่านจากการค้นคว้าข้อมูลที่เกี่ยวข้อง - ประเมินจากรายงานที่นักศึกษาได้รับมอบหมายให้จัดทำและนำเสนอรายงานในชั้นเรียน

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	วิธีการสอนที่จะใช้พัฒนาการเรียนรู้	วิธีการวัดและประเมินผล
- สามารถวิเคราะห์การรักษาความมั่นคงและบริหารความเสี่ยงระบบสารสนเทศให้ตรงตามข้อกำหนดได้ - สามารถติดตามความก้าวหน้าและวิวัฒนาการของการรักษาความมั่นคงและบริหารความเสี่ยงระบบสารสนเทศทั้งการนำไปประยุกต์ - รู้ เข้าใจและสนใจพัฒนาความรู้ความชำนาญทางการรักษาความมั่นคงและบริหารความเสี่ยงระบบสารสนเทศอย่างต่อเนื่อง		
3. ทักษะทางปัญญา - คิดอย่างมีวิจารณญาณและอย่างเป็นระบบ - สามารถสืบค้น ตีความ และประเมิน เพื่อใช้ในการแก้ไขปัญหาอย่างสร้างสรรค์ - สามารถรวบรวม ศึกษา วิเคราะห์และสรุปประเด็นปัญหาและความต้องการ - สามารถประยุกต์ความรู้และทักษะกับการแก้ไขปัญหาทางการรักษาความมั่นคงและบริหารความเสี่ยงระบบสารสนเทศได้อย่างเหมาะสม	- วิเคราะห์จากกรณีศึกษาหรือจากปัญหาที่เกิดขึ้นจริง - ศึกษาค้นคว้างานหรือบทความที่เกี่ยวข้อง	- ประเมินผลจาการทดสอบย่อยในชั้นเรียน - สอบกลางภาคและปลายภาคโดยเน้นข้อสอบที่มีการวิเคราะห์โจทย์ -

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	วิธีการสอนที่จะใช้พัฒนาการเรียนรู้	วิธีการวัดและประเมินผล
4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ - มีความรับผิดชอบในการกระทำของตนเองและรับผิดชอบงานในกลุ่ม และมีการพัฒนาการเรียนรู้ทั้งของตนเองและทางวิชาชีพอย่างต่อเนื่อง	- จัดกิจกรรมกลุ่มในการวิเคราะห์โจทย์กรณีศึกษา และการนำเสนอวิธีแก้ปัญหา - มอบหมายงานรายกลุ่ม และรายบุคคล	- ประเมินตนเอง และเพื่อน ด้วยแบบฟอร์มที่กำหนด - รายงานที่นำเสนอ พฤติกรรมการทำงานเป็นทีม
5. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ - สามารถแนะนำประเด็นการแก้ไขปัญหาโดยใช้โครงสร้างข้อมูลและอัลกอริทึมหรือการประยุกต์ต่อปัญหาที่เกี่ยวข้องอย่างสร้างสรรค์ - สามารถสื่อสารอย่างมีประสิทธิภาพทั้งปากเปล่าและการเขียน เลือกใช้รูปแบบของสื่อการนำเสนออย่างเหมาะสม	- จัดกิจกรรมการเรียนรู้ในรายวิชา ให้นักศึกษาได้วิเคราะห์และค้นคว้าด้วยตนเอง โดยเน้นแหล่งที่มาของข้อมูลที่น่าเชื่อถือ - นำเสนอโดยใช้รูปแบบและเทคโนโลยีที่เหมาะสม	- ประเมินจากเทคนิคการการจัดทำรายงาน และนำเสนอด้วยสื่อเทคโนโลยี การมีส่วนร่วมในการอภิปรายและวิธีการอภิปราย - ประเมินจากความสามารถในการอธิบาย ถึงข้อจำกัด เหตุผลในการเลือกใช้เครื่องมือต่างๆ การอภิปราย กรณีศึกษาต่างๆ ที่มีการนำเสนอต่อชั้นเรียน

หมวดที่ 5 แผนการสอนและการประเมินผล

1. แผนการสอน

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
1	ความรู้เบื้องต้นเกี่ยวกับอาชญากรรมไซเบอร์	4	ทฤษฎี: บรรยายภาพรวม ความหมาย ความสำคัญ ปฏิบัติ: วิเคราะห์ข่าวหรือกรณีศึกษาจริงเกี่ยวกับอาชญากรรมไซเบอร์	รศ.เอกรินทร์
2	กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์	4	ทฤษฎี: ศึกษาพ.ร.บ. คอมพิวเตอร์ และกฎหมายสากล ปฏิบัติ: วิเคราะห์เหตุการณ์โดยใช้หลักกฎหมาย	รศ.เอกรินทร์
3	ประเภทของอาชญากรรมไซเบอร์	4	ทฤษฎี: อธิบายชนิด เช่น Hacking, Phishing, Ransomware ปฏิบัติ: จัดกลุ่มวิเคราะห์กรณีศึกษาตามประเภทอาชญากรรม	รศ.เอกรินทร์
4	ขั้นตอนการสืบสวนอาชญากรรมทางคอมพิวเตอร์	4	ทฤษฎี: อธิบายกระบวนการ Digital Investigation ปฏิบัติ: จำลองสถานการณ์การเกิดเหตุ และกำหนดแนวทางการสืบสวน	รศ.เอกรินทร์
5	หลักการเก็บรวบรวมหลักฐานดิจิทัล	4	ทฤษฎี: ความสำคัญ ความถูกต้องตามกฎหมาย ปฏิบัติ: ฝึกเขียน Chain of Custody	รศ.เอกรินทร์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
6	ภาพรวมของการพิสูจน์หลักฐานดิจิทัล	4	ทฤษฎี: นิยาม กระบวนการ และแนวคิดทาง Forensics ปฏิบัติ: วิเคราะห์แผนภาพการพิสูจน์หลักฐานจากสถานการณ์จริง	รศ.เอกรินทร์
7	ระบบไฟล์ของระบบปฏิบัติการต่าง ๆ	4	ทฤษฎี: FAT32, NTFS, EXT4 ปฏิบัติ: ใช้โปรแกรม Forensic Tools วิเคราะห์ระบบไฟล์ตัวอย่าง	รศ.เอกรินทร์
8	สอบกลางภาค	2 ชม.		รศ.เอกรินทร์
9	การวิเคราะห์หลักฐานจากระบบปฏิบัติการ	4	ทฤษฎี: จุดที่มักถูกโจมตี Log Files, Registry ปฏิบัติ: ตรวจสอบ Log จากระบบจำลอง เช่น Windows Event Viewer	รศ.เอกรินทร์
10	เครื่องมือที่ใช้ในการพิสูจน์หลักฐานดิจิทัล	4	ทฤษฎี: แนะนำเครื่องมือ เช่น Autopsy, FTK, Wireshark ปฏิบัติ: ทดลองใช้งาน Autopsy ตรวจไฟล์จาก Disk Image	รศ.เอกรินทร์
11	การเก็บหลักฐานจากระบบเครือข่าย	4	ทฤษฎี: Packet Capture, Network Traffic ปฏิบัติ: ใช้ Wireshark จับแพ็กเกต และวิเคราะห์เบื้องต้น	รศ.เอกรินทร์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
12	การวิเคราะห์หลักฐานจากการโจมตีระบบเครือข่าย	4	ทฤษฎี: เทคนิคการโจมตี เช่น DDoS, Man-in-the-Middle ปฏิบัติ: วิเคราะห์แพ็กเกตที่เกิดจากการโจมตีจำลอง	รศ.เอกรินทร์
13	การป้องกันและตอบสนองต่อเหตุการณ์ไซเบอร์	4	ทฤษฎี: Incident Response Plan ปฏิบัติ: วางแผนตอบสนองเหตุการณ์โจมตีในระบบจำลอง	รศ.เอกรินทร์
14	การจัดทำรายงานการพิสูจน์หลักฐาน	4	ทฤษฎี: โครงสร้างรายงานหลักฐานที่เหมาะสม ปฏิบัติ: เขียนรายงานสืบสวนจากเหตุการณ์จำลอง	รศ.เอกรินทร์
15	กรณีศึกษาการสืบสวนอาชญากรรมไซเบอร์	4	ทฤษฎี: วิเคราะห์เหตุการณ์จริงจากข่าวหรือองค์กร ปฏิบัติ: แบ่งกลุ่มอภิปรายและสรุปผล	รศ.เอกรินทร์
16	สอบปลายภาค	2 ชม.		

2. แผนการประเมินผลการเรียนรู้

ผลการเรียนรู้ (Learning Outcome)	วิธีการประเมิน	กำหนดเวลาการประเมิน (สัปดาห์ที่)	สัดส่วนของการประเมินผล
1.2, 1.3, 1.4, 2.1,	- สอบกลางภาค	8	20%

2.2, 2.3, 2.4, 2.5, 3.1-3.4, 4.1,4.6	- นำเสนอรายงานกลุ่มตามที่ได้รับมอบหมาย - สอบปลายภาค	7, 15 16	20% 30%
1.2, 1.3, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1-3.4, 4.1,4.6, 5.1-5.4	การส่งงานตามที่มอบหมายรายบุคคลและรายกลุ่ม	ตลอดภาคการศึกษา	30%

หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

1. เอกสารและตำราหลัก

เอกรินทร์ วทัญญูเลิศสกุล, “ความมั่นคงในเครือข่ายคอมพิวเตอร์”, อุบลราชธานี : มหาวิทยาลัยราชภัฏอุบลราชธานี, 2562.

เดชานุชิต กตัญญูทวีทิพย์, “การสื่อสารและเครือข่ายคอมพิวเตอร์” สำนักพิมพ์ซีเอ็ดยูเคชั่นจำกัด, 2548.

2. เอกสารและข้อมูลสำคัญ

3. **เอกสารและข้อมูลแนะนำ**

ก่อกิจ วีระอาชากุล, “ติดตั้งและปรับแต่งเซิร์ฟเวอร์ Linux”, กรุงเทพฯ : สำนักพิมพ์อินโฟเพรส, 2548.

สุรศักดิ์ สงวนพงษ์, “สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี”, สำนักพิมพ์ซีเอ็ดยูเคชั่นจำกัด, 2545.

โอภาส เอี่ยมสิริวงศ์, “เครือข่ายคอมพิวเตอร์การสื่อสาร”, สำนักพิมพ์ซีเอ็ดยูเคชั่นจำกัด, 2549.

หมวดที่ 7 การประเมินรายวิชาและกระบวนการปรับปรุง

1. กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนักศึกษา

การประเมินประสิทธิผลในรายวิชานี้ ที่จัดทำโดยนักศึกษา ได้จัดกิจกรรมในการนำแนวคิดและความเห็นจากนักศึกษาได้ดังนี้

- การสนทนากลุ่มระหว่างผู้สอนและผู้เรียน
- การสังเกตการณ์จากพฤติกรรมของผู้เรียน
- แบบประเมินผู้สอน และแบบประเมินรายวิชา

2. กลยุทธ์การประเมินการสอน

- การสังเกตการณ์สอนของผู้ร่วมทีมการสอน
- ผลการสอบ
- การทวนสอบผลประเมินการเรียนรู้
- ผลที่ได้จากการทำงานตามที่ได้รับมอบหมาย

3. การปรับปรุงการสอน

หลังจากผลการประเมินการสอนในข้อ 2 จึงมีการปรับปรุงการสอน โดยการจัดกิจกรรมในการระดมสมอง และหาข้อมูลเพิ่มเติมในการปรับปรุงการสอน ดังนี้

- สัมมนาการจัดการเรียนการสอน
- การวิจัยในและนอกชั้นเรียน

4. การทวนสอบมาตรฐานผลสัมฤทธิ์รายวิชาของนักศึกษา

ในระหว่างกระบวนการสอนรายวิชา มีการทวนสอบผลสัมฤทธิ์ในรายหัวข้อ รวมถึงพิจารณาจากผลที่ได้จากการทำงานตามที่ได้รับมอบหมาย และหลังการออกผลการเรียนรายวิชา มีการทวนสอบผลสัมฤทธิ์โดยรวมในวิชาดังนี้

- การทวนสอบการให้คะแนนจากการสุ่มตรวจผลงานของนักศึกษาโดยอาจารย์อื่น หรือผู้ทรงคุณวุฒิ ที่ไม่ใช่อาจารย์ประจำหลักสูตร
- มีการตั้งคณะกรรมการในกลุ่มวิชา ตรวจสอบผลการประเมินการเรียนรู้ของนักศึกษา โดยตรวจสอบข้อสอบ รายงาน วิธีการให้คะแนนสอบ และการให้คะแนนพฤติกรรม

5. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา

จากผลการประเมิน และทวนสอบผลสัมฤทธิ์ประสิทธิผลรายวิชา ได้มีการวางแผนการปรับปรุงการสอน และรายละเอียดวิชา เพื่อให้เกิดคุณภาพมากขึ้น ดังนี้

- ปรับปรุงรายวิชาทุก 3 ปี หรือ ตามข้อเสนอแนะและผลการทวนสอบมาตรฐานผลสัมฤทธิ์ตามข้อ 4
- เปลี่ยนหรือสลับอาจารย์ผู้สอน เพื่อให้นักศึกษามีมุมมองในเรื่องการประยุกต์ความรู้นี้กับปัญหาที่มาจากงานวิจัยของอาจารย์หรือแหล่งข้อมูลต่าง ๆ ที่เกี่ยวข้องกับในรายวิชา