บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในอดีตการพัฒนาการติดต่อสื่อสารของมนุษย์ที่พัฒนามาเป็นลำดับ จะอยู่บนพื้นฐานของการแก้ไขข้อบกพร่องหรืออุปสรรคในความไม่สะดวกของเวลาและระยะทาง ซึ่งเป็นเหตุผลที่ในปัจจุบันจะพบเห็นเครื่องมือหลายชนิดที่ถูกสร้างขึ้นเพื่อใช้ในการอำนวยความสะดวกและลดอุปสรรค ดังกล่าว เช่น โทรศัพท์ โทรสาร และพัฒนาต่อมาจนกระทั่งมาถึงยุคของคอมพิวเตอร์ในปัจจุบัน ความก้าวหน้าทางเทคโนโลยี ได้พัฒนาความสามารถของคอมพิวเตอร์ ซึ่งจากเดิมที่มีวัตถุประสงค์เพื่อช่วยในการประมวลผลเพียงอย่างเดียว ให้สามารถใช้เป็นเครื่องมือในการติดต่อสื่อสารที่รวดเร็วและมีประสิทธิภาพในปัจจุบัน โดยสามารถติดต่อกันได้ด้วยภาพและเสียงระหว่างสถานที่สองแห่งหรือที่เรียกว่าระบบเครือข่าย (Networks) และสามารถติดต่อเชื่อมโยงกันไม่เพียงเฉพาะภายในหน่วยงานหรือส่วนบุคคล แต่สามารถใช้ในการติดต่อได้ในระดับระหว่างประเทศและพัฒนาเป็นระบบเครือข่ายระดับโลกหรือที่เรียกว่า การสื่อสารทาง อินเทอร์เน็ต (internet) หรือทางด่วนข้อมูลในปัจจุบัน

จากการเปิดกว้างของข้อมูลซึ่งบุคคลทั่วโลกสามารถที่จะเข้าสู่ระบบคอมพิวเตอร์ได้ นำมาซึ่งการตระหนักถึงระบบการรักษาข้อมูลซึ่งเป็นความลับภายในหน่วยงานต่างๆเพื่อป้องกันการเข้าไปกระทำการอันใดโดยมิชอบ ที่เรียกว่าระบบรักษาความปลอดภัย (Security system) ซึ่งการรักษาความปลอดภัยของระบบคอมพิวเตอร์นี้มีด้วยกันหลายประการ ตัวอย่างเช่น การกำหนดรหัสผ่าน (passwords) และการเข้ารหัส (encryption) เป็นต้น

แฮกเกอร์ (Hacker) เป็นคำที่จะได้ยินบ่อยครั้งเมื่อมีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การโจรกรรมข้อมูลทางคอมพิวเตอร์ การปล่อยไวรัสคอมพิวเตอร์เพื่อทำลายระบบคอมพิวเตอร์ หรือการเจาะระบบคอมพิวเตอร์ของหน่วยงานที่มีความสำคัญต่างๆ แต่ถ้าถามว่าแฮกเกอร์คือใคร มีโอกาสเป็นไปได้มากที่จะได้รับคำตอบหรือความคิดเห็นที่แตกต่างกัน ที่เป็นเช่นนี้เพราะคำว่าแฮกเกอร์เป็นคำที่ถูกนำไปใช้อย่างฟุ่มเฟือยจนกระทั่งไม่สามารถทราบได้แน่ชัดว่าแฮกเกอร์มีความหมายเช่นใด

ปัญหาดังกล่าวจึงเป็นสาเหตุที่ทำให้ผู้เขียนมีความสนใจศึกษาเพื่อหาคำตอบที่ถูกต้อง ซึ่งนอกจากปัญหาในเรื่องการให้ความหมายของแฮกเกอร์ดังกล่าวแล้ว ยังมีปัญหาที่สืบเนื่องต่อมาคือ ปัญหาที่ว่าการกระทำของแฮกเกอร์นั้นจะมีเหตุสมควรเพียงพอหรือไม่ที่จะกำหนด

ให้เป็นความผิดทางอาญา และหากว่าการกระทำของแฮกเกอร์มีเหตุผลเพียงพอที่จะกำหนดเป็นความผิดทางอาญาแล้ว รัฐจะมีนโยบายทางอาญาประการใดต่อผู้มีความประพฤติเช่นนี้ นอกจากนี้การกระทำความผิดทางคอมพิวเตอร์ก่อให้เกิดปัญหาการปรับบทกฎหมายที่มีอยู่ในปัจจุบัน ซึ่งจำเป็นต้องอาศัยการศึกษาค้นคว้าต่อไป จะมีแนวความคิดหรือแนวทางใดหรือไม่ที่สามารถใช้เป็นแนวทางในการป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในอนาคต

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาถึงความหมายและลักษณะการกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

๒. เพื่อศึกษาหาเหตุผลในการสนับสนุนให้การกระทำของผู้เจาะระบบคอมพิวเตอร์เป็นความผิดอาญา

๓. เพื่อศึกษาแนวนโยบายทางอาญาต่อผู้เจาะระบบคอมพิวเตอร์

๔. เพื่อศึกษาและพัฒนาแนวความคิดในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา

ประโยชน์ที่คาดว่าจะได้รับ

๑. เพื่อเป็นแนวทางแก่กระบวนการยุติธรรมในประเทศไทยในการเตรียมความพร้อมเพื่อรับมือกับการเจาะระบบคอมพิวเตอร์

๒. เพื่อเป็นแนวทางแก่รัฐในการกำหนดนโยบายทางอาญาแก่ผู้เจาะระบบคอมพิวเตอร์

๓. เป็นการกระตุ้นให้ผู้มีหน้าที่เกี่ยวข้องในการปราบปรามอาชญากรรมให้ความสนใจการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มากขึ้น

วิธีการดำเนินการวิจัย

การศึกษาวิจัยนี้จะใช้การวิจัยจากเอกสารทั้งที่เป็นเอกสารภาษาไทยและภาษาต่างประเทศ ตลอดจนข้อมูลจากอินเทอร์เน็ต เพื่อรวบรวมเป็นเหตุผลสนับสนุนตามแนวคิดของผู้ทำการวิจัยและหาคำตอบต่อปัญหาหรือข้อโต้แย้งที่เกิดขึ้น

สมมุติฐานของการวิจัย

การเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต สามารถก่อให้เกิดความเสียหายได้อย่างมากมายแก่ระบบคอมพิวเตอร์ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือของหน่วยงานต่างๆ เหตุนี้เพื่อเป็นการป้องกันและปราบปรามการกระทำความผิดที่อาจเกิดขึ้น หลังจากที่มีการเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตแล้ว เช่นการถ่ายเทข้อมูล การแก้ไขเปลี่ยนแปลงและการทำลายข้อมูล เป็นต้น จึงสมควรกำหนดให้การแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นการกระทำที่เป็นความผิดอาญา