[Chương I 1](#_Toc200695806)

[NHỮNG QUY ĐỊNH CHUNG 1](#_Toc200695807)

[Điều 1. Phạm vi điều chỉnh 1](#_Toc200695808)

[Điều 2. Đối tượng áp dụng 1](#_Toc200695809)

[Điều 3. Giải thích từ ngữ 1](#_Toc200695810)

[Điều 4. Chính sách của Nhà nước về an ninh mạng 3](#_Toc200695811)

[Điều 5. Nguyên tắc bảo vệ an ninh mạng 3](#_Toc200695812)

[Điều 6. Biện pháp bảo vệ an ninh mạng 4](#_Toc200695813)

[Điều 7. Bảo vệ không gian mạng quốc gia 4](#_Toc200695814)

[Điều 8. Hợp tác quốc tế về an ninh mạng 4](#_Toc200695815)

[Điều 9. Các hành vi bị nghiêm cấm về an ninh mạng 5](#_Toc200695816)

[Điều 10. Xử lý vi phạm pháp luật về an ninh mạng 6](#_Toc200695817)

[Chương II 6](#_Toc200695818)

[HOẠT ĐỘNG BẢO ĐẢM AN NINH MẠNG 6](#_Toc200695819)

[MỤC 1: 6](#_Toc200695820)

[BẢO VỆ THÔNG TIN MẠNG 6](#_Toc200695821)

[Điều 11. Phân loại thông tin 6](#_Toc200695822)

[Điều 12. Quản lý gửi thông tin trên mạng 7](#_Toc200695823)

[Điều 13. Bảo đảm an ninh thông tin trên không gian mạng 7](#_Toc200695824)

[Điều 14. Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo vệ thông tin mạng 8](#_Toc200695825)

[MỤC 2: 8](#_Toc200695826)

[BẢO VỆ HỆ THỐNG THÔNG TIN 8](#_Toc200695827)

[Điều 15. Phân loại cấp độ hệ thống thông tin 8](#_Toc200695828)

[Điều 16. Nhiệm vụ bảo vệ hệ thống thông tin 8](#_Toc200695829)

[Điều 17. Biện pháp bảo vệ hệ thống thông tin 9](#_Toc200695830)

[Điều 18. Danh mục hệ thống thông tin quan trọng quốc gia 9](#_Toc200695831)

[Điều 19. Trách nhiệm bảo đảm an ninh mạng cho hệ thống thông tin quan trọng quốc gia 10](#_Toc200695832)

[MỤC 3: 11](#_Toc200695833)

[PHÒNG NGỪA, XỬ LÝ HÀNH VI XÂM PHẠM AN NINH MẠNG 11](#_Toc200695834)

[Điều 20. Phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế 11](#_Toc200695835)

[Điều 21. Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng 12](#_Toc200695836)

[Điều 22. Phòng, chống xâm hại trẻ em trên không gian mạng 14](#_Toc200695837)

[Điều 23. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại 14](#_Toc200695838)

[Điều 24. Phòng, chống tấn công mạng 15](#_Toc200695839)

[Điều 25. Phòng, chống khủng bố mạng 16](#_Toc200695840)

[Điều 26. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng 16](#_Toc200695841)

[Điều 27. Đấu tranh bảo vệ an ninh mạng 17](#_Toc200695842)

[Điều 28. Ngăn chặn xung đột thông tin trên mạng 17](#_Toc200695843)

[CHƯƠNG III 18](#_Toc200695844)

[PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO 18](#_Toc200695845)

[Điều 29. Phòng, chống tội phạm sử dụng không gian mạng trong lĩnh vực sản xuất, kinh doanh, thương mại và sở hữu trí tuệ 18](#_Toc200695846)

[Điều 30. Phòng, chống tội phạm sử dụng không gian mạng trong lĩnh vực thuế, tài chính, ngân hàng, chứng khoán, bảo hiểm 19](#_Toc200695847)

[Điều 31. Phòng, chống tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông 20](#_Toc200695848)

[Điều 32. Phòng ngừa, xử lý hành vi sử dụng công nghệ cao xâm phạm trật tự xã hội 21](#_Toc200695849)

[Điều 33. Thẩm quyền của lực lượng chuyên trách bảo vệ an ninh mạng trong phòng, chống tội phạm sử dụng công nghệ cao. 21](#_Toc200695850)

[Điều 34. Trách nhiệm của nhà cung cấp dịch vụ, tổ chức, cá nhân sử dụng dịch vụ đấu tranh phòng, chống tội phạm sử dụng công nghệ cao 22](#_Toc200695851)

[Chương IV 23](#_Toc200695852)

[TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN NINH MẠNG 23](#_Toc200695853)

[Điều 35. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng 23](#_Toc200695854)

[Điều 36. Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng 23](#_Toc200695855)

[Điều 37. Đánh giá hợp chuẩn, hợp quy về an ninh mạng 24](#_Toc200695856)

[Chương V 25](#_Toc200695857)

[SẢN PHẨM, DỊCH VỤ AN NINH MẠNG 25](#_Toc200695858)

[MỤC 1: 25](#_Toc200695859)

[CẤP GIẤY PHÉP KINH DOANH SẢN PHẨM, DỊCH VỤ AN NINH MẠNG 25](#_Toc200695860)

[Điều 38. Sản phẩm, dịch vụ an ninh mạng 25](#_Toc200695861)

[Điều 39. Điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng 26](#_Toc200695862)

[Điều 40. Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng 27](#_Toc200695863)

[MỤC 2: 27](#_Toc200695864)

[QUẢN LÝ NHẬP KHẨU SẢN PHẨM AN NINH MẠNG 27](#_Toc200695865)

[Điều 41. Nguyên tắc quản lý nhập khẩu sản phẩm an ninh mạng 27](#_Toc200695866)

[Điều 42. Sản phẩm nhập khẩu theo giấy phép trong lĩnh vực an ninh mạng 28](#_Toc200695867)

[Chương VI 28](#_Toc200695868)

[ĐIỀU KIỆN BẢO ĐẢM AN NINH MẠNG 28](#_Toc200695869)

[Điều 43. Nghiên cứu, phát triển an ninh mạng 28](#_Toc200695870)

[Điều 44. Nâng cao năng lực tự chủ về an ninh mạng 29](#_Toc200695871)

[Điều 45. Lực lượng bảo vệ an ninh mạng 29](#_Toc200695872)

[Điều 46. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng 29](#_Toc200695873)

[Điều 47. Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng 30](#_Toc200695874)

[Điều 48. Giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng 30](#_Toc200695875)

[Điều 49. Phổ biến kiến thức về an ninh mạng 30](#_Toc200695876)

[Điều 50. Kinh phí bảo vệ an ninh mạng 30](#_Toc200695877)

[Điều 51. Văn bằng, chứng chỉ đào tạo về an ninh mạng 30](#_Toc200695878)

[CHƯƠNG VII 31](#_Toc200695879)

[QUẢN LÝ NHÀ NƯỚC VỀ AN NINH MẠNG 31](#_Toc200695880)

[Điều 52. Nội dung quản lý nhà nước về an ninh mạng 31](#_Toc200695881)

[Điều 53. Trách nhiệm quản lý nhà nước về an ninh mạng 31](#_Toc200695882)

[Điều 54. Trách nhiệm của chủ quản hệ thống thông tin 32](#_Toc200695883)

[Điều 55. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng 32](#_Toc200695884)

[Điều 56. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng 32](#_Toc200695885)

[Chương VIII 33](#_Toc200695886)

[ĐIỀU KHOẢN THI HÀNH 33](#_Toc200695887)

[Điều 57. Điều khoản chuyển tiếp 33](#_Toc200695888)

[Điều 58. Hiệu lực thi hành 34](#_Toc200695889)

|  |  |
| --- | --- |
| **QUỐC HỘI** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc** |
| Luật số: …../2025/QH15 |  |

**LUẬT**

**Dự thảo lần 4**

**AN NINH MẠNG**

*Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam;*

*Quốc hội ban hành Luật An ninh mạng.*

**Chương I**

**NHỮNG QUY ĐỊNH CHUNG**

# **Phạm vi điều chỉnh**

Luật này quy định về hoạt động bảo đảm an ninh mạng nhằm bảo vệ chủ quyền không gian mạng quốc gia, bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân khi tham gia không gian mạng, bao gồm: bảo vệ thông tin mạng, bảo vệ hệ thống thông tin; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; phòng, chống tội phạm sử dụng công nghệ cao; tiêu chuẩn, quy chuẩn an ninh mạng; sản phẩm, dịch vụ an ninh mạng; điều kiện bảo đảm an ninh mạng; quản lý nhà nước về an ninh mạng và trách nhiệm của các chủ thể trong việc tuân thủ quy định pháp luật về an ninh mạng.

# **Đối tượng áp dụng**

Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến các hoạt động trên không gian mạng tại Việt Nam.

# **Giải thích từ ngữ**

Trong Luật này, các từ ngữ dưới đây được hiểu như sau:

1. *An ninh mạng* là sự bảo đảm an toàn, ổn định, bền vững của thông tin, hệ thống thông tin, không gian mạng và phòng, chống các hoạt động trên không gian mạng gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

4. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng.

5. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

6. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

7. *Phần cứng độc hại* là các bộ phận vật lý của hệ thống máy tính, hệ thống thông tin có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống máy tính, hệ thống thông tin hoặc thực hiện các hoạt động không được quyền đối với dữ liệu lưu trữ trong hệ thống thông tin.

8. *Nhật ký hệ thống* là hệ thống được thiết lập có chức năng ghi nhận, lưu trữ và có thể trích xuất dữ liệu phản ánh những sự kiện liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh mạng của hệ thống và dữ liệu do người dùng tạo ra trong quá trình sử dụng hệ thống, truy cập dịch vụ Internet.

9. *Tội phạm sử dụng công nghệ cao* là hành vi nguy hiểm cho xã hội quy định trong Bộ luật Hình sự được thực hiện thông qua việc sử dụng công nghệ thông tin, mạng máy tính, Internet hoặc các thiết bị số nhằm mục đích lừa đảo, chiếm đoạt tài sản, xâm nhập hệ thống máy tính, phát tán thông tin độc hại hoặc gây thiệt hại cho cá nhân, tổ chức và xã hội.

10. *Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của không gian mạng.

11. *Khủng bố mạng* là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.

12. *Gián điệp mạng* là hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia nhằm chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên không gian mạng của cơ quan, tổ chức, cá nhân Việt Nam.

13. *Tài sản số* là sản phẩm công nghệ số được tạo ra, phát hành, chuyển giao và xác thực quyền sở hữu bằng công nghệ chuỗi khối, có giá và quyền tài sản theo quy định của pháp luật về dân sự và pháp luật có liên quan*.*

14. *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

15.*Xung đột thông tin*là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

16. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

17. *Sản phẩm an ninh mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin và không gian mạng.

18. *Dịch vụ an ninh mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin và không gian mạng.

19. *Nhà cung cấp dịch vụ* là các doanh nghiệp, tổ chức, các nhân cung cấp các sản phẩm, dịch vụ trên không gian mạng, gồm: dịch vụ Internet (ISP), dịch vụ bưu chính, viễn thông, dịch vụ lưu trữ, máy chủ, tên miền, mạng riêng ảo (Virtual Private Network), máy chủ trung gian (Proxy), dịch vụ điện toán đám mây (Cloud Computing), mạng xã hội, trang thông tin điện tử, dịch vụ viễn thông, các tổ chứ tài chính, tín dụng, ngân hàng, chi nhánh ngân hàng nước ngoài tại Việt Nam, ví điện tử, trung gian thanh toán, các sản giao dịch chứng khoán, sàn giao dịch tài sản số, sàn thương mại điện tử, dịch vụ vận chuyển (logistic), truyền hình số, trò chơi trực tuyến và các loại sản phẩm, dịch vụ khác trên không gian mạng.

# **Chính sách của Nhà nước về an ninh mạng**

1. Ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại.

2. Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng.

4. Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng.

5. Tăng cường hợp tác quốc tế về an ninh mạng.

# **Nguyên tắc bảo vệ an ninh mạng**

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm an ninh, chủ quyền quốc gia, lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.

4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.

5. Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng quốc gia.

6. Hệ thống thông tin quan trọng quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

7. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

# **Biện pháp bảo vệ an ninh mạng**

1. Biện pháp bảo vệ an ninh mạng bao gồm:

a) Biện pháp khoa học - kỹ thuật;

b) Biện pháp hành chính;

c) Biện pháp nghiệp vụ;

d) Biện pháp điều tra, truy tố;

e) Các biện pháp khác theo quy định của pháp luật.

2. Chính phủ quy định chi tiết về các biện pháp bảo vệ an ninh mạng.

# **Bảo vệ không gian mạng quốc gia**

1. Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

2. Cơ sở hạ tầng không gian mạng quốc gia là hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng quốc gia.

3. Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia, cơ sở hạ tầng không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.

# **Hợp tác quốc tế về an ninh mạng**

1. Hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng, cùng có lợi và tuân thủ Hiến pháp, pháp luật Việt Nam, điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên..

2. Nội dung hợp tác quốc tế về an ninh mạng bao gồm:

a) Chia sẻ thông tin, dữ liệu và cảnh báo sớm về nguy cơ, sự cố, tấn công mạng ảnh hưởng đến an ninh mạng;

b) Xây dựng khuôn khổ pháp lý, chính sách và cơ chế phối hợp trong bảo vệ an ninh mạng; ký kết, thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng;

c) Đào tạo, tư vấn, chia sẻ kinh nghiệm và nâng cao năng lực chuyên môn, kỹ thuật trong lĩnh vực an ninh mạng;

d) Phòng, chống tội phạm sử dụng công nghệ cao; phối hợp điều tra, xử lý vi phạm pháp luật và tội phạm sử dụng công nghệ cao có yếu tố nước ngoài;

đ) Nghiên cứu, phát triển, chuyển giao công nghệ, sản phẩm, giải pháp kỹ thuật phục vụ công tác bảo vệ an ninh mạng;

e) Tổ chức hội nghị, hội thảo, diễn đàn quốc tế và triển khai các chương trình, dự án hợp tác quốc tế về an ninh mạng;

g) Hoạt động hợp tác quốc tế khác về an ninh mạng.

# **Các hành vi bị nghiêm cấm về an ninh mạng**

1. Sử dụng không gian mạng để thực hiện hành vi sau đây:

a) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm lãnh tụ, anh hùng dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

c) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng và các thông tin có nội dung vi phạm pháp luật khác;

đ) Xúi giục, lôi kéo, kích động người khác phạm tội.

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm sử dụng công nghệ cao.

3. Thực hiện các hành vi sau đây:

a) Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng;

b) Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an ninh mạng của hệ thống thông tin;

c) Tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin;

d) Phát tán thư rác, nội dung vi phạm quy định về quảng cáo, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo;

đ) Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin cá nhân của người khác;

e) Lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân;

g) Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân;

h) Tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự;

i) Sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

4. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của không gian mạng; phát tán chương trình tin học gây hại cho hoạt động của không gian mạng; xâm nhập trái phép vào thông tin, hệ thống thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

5. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

6. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

7. Hành vi khác vi phạm quy định của Luật này.

# **Xử lý vi phạm pháp luật về an ninh mạng**

Chủ thể có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

**Chương II**

**HOẠT ĐỘNG BẢO ĐẢM AN NINH MẠNG**

**MỤC 1:**

**BẢO VỆ THÔNG TIN MẠNG**

# **Phân loại thông tin**

1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp.

2. Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Cơ quan, tổ chức sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải có trách nhiệm xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

# **Quản lý gửi thông tin trên mạng**

1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin;

b) Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật.

3. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ ứng dụng viễn thông và doanh nghiệp cung cấp dịch vụ công nghệ thông tin gửi thông tin có trách nhiệm sau đây:

a) Tuân thủ quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của tổ chức, cá nhân;

b) Áp dụng biện pháp ngăn chặn, xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật;

c) Có phương thức để người tiếp nhận thông tin có khả năng từ chối việc tiếp nhận thông tin;

d) Cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ quản lý, bảo đảm an ninh mạng khi có yêu cầu.

# **Bảo đảm an ninh thông tin trên không gian mạng**

1. Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin có nội dung xâm phạm an ninh quốc gia, trật tự an toàn xã hội được quy định khoản 1, 2, 3, 4, 5 Điều 20 Luật này.

2. Doanh nghiệp trong nước và nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm sau đây:

a) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản hoặc thư điện tử, điện thoại hoặc một loại hình thức trao đổi khác đã được xác nhận để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng;

b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm pháp luật trên dịch vụ, kho ứng dụng hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ;

c) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung quy định tại khoản 1, 2, 3, 4, 5 Điều 20 của Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.

3. Doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu cá nhân của công dân Việt Nam thì thực hiện theo quy định của Luật Bảo vệ dữ liệu cá nhân.

# **Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo vệ thông tin mạng**

1. Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo vệ thông tin mạng.

2. Cơ quan, tổ chức, cá nhân sử dụng dịch vụ trên mạng có trách nhiệm thông báo kịp thời cho doanh nghiệp cung cấp dịch vụ hoặc bộ phận chuyên trách ứng cứu sự cố khi phát hiện các hành vi phá hoại hoặc sự cố an ninh mạng.

**MỤC 2:**

**BẢO VỆ HỆ THỐNG THÔNG TIN**

# **Phân loại cấp độ hệ thống thông tin**

1. Phân loại cấp độ hệ thống thông tin là việc xác định cấp độ an ninh mạng của hệ thống thông tin, bao gồm:

a) Cấp độ 1 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

b) Cấp độ 2 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại nghiêm trọng tới lợi ích công cộng hoặc làm tổn hại tới trật tự, an toàn xã hội;

c) Cấp độ 3 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng, trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia.

2. Hệ thống thông tin cấp độ 3 là hệ thống thông tin quan trọng quốc gia.

3. Chính phủ quy định chi tiết tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin và trách nhiệm bảo đảm an ninh mạng theo từng cấp độ.

# **Nhiệm vụ bảo vệ hệ thống thông tin**

Nội dung nhiệm vụ bảo vệ hệ thống thông tin, bao gồm:

1. Xác định cấp độ an ninh mạng của hệ thống thông tin.

2. Đánh giá và quản lý rủi ro an ninh hệ thống thông tin.

3. Đôn đốc, giám sát, kiểm tra công tác bảo vệ hệ thống thông tin.

4. Tổ chức triển khai các biện pháp bảo vệ hệ thống thông tin.

5. Thực hiện chế độ báo cáo theo quy định.

6. Tổ chức tuyên truyền, nâng cao nhận thức về an ninh mạng.

# **Biện pháp bảo vệ hệ thống thông tin**

Các biện pháp bảo vệ hệ thống thông tin, bao gồm:

1. Ban hành quy định về bảo đảm an ninh mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin.

2. Áp dụng biện pháp quản lý, kỹ thuật theo tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng để phòng, chống nguy cơ, khắc phục sự cố an ninh mạng.

3. Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng.

4. Thực hiện giám sát an ninh mạng.

# **Danh mục hệ thống thông tin quan trọng quốc gia**

1. Danh mục hệ thống thông tin quan trọng quốc gia là danh sách hệ thống thông tin quan trọng quốc gia được xác lập, ban hành và áp dụng biện pháp bảo vệ tương xứng nhằm đảm bảo hoạt động ổn định của các lĩnh vực quan trọng, bao gồm:

a) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu;

b) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước;

c) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng;

d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái;

đ) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia;

e) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương;

g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí;

h) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

2. Thủ tướng Chính phủ ban hành và sửa đổi, bổ sung Danh mục hệ thống thông tin quan trọng quốc gia.

# **Trách nhiệm bảo đảm an ninh mạng cho hệ thống thông tin quan trọng quốc gia**

1. Chủ quản hệ thống thông tin quan trọng quốc gia có trách nhiệm sau đây:

a) Thực hiện quy định tại Điều 16, 17 Luật này;

b) Kiểm tra an ninh mạng trong trường hợp đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng; khi có thay đổi hiện trạng hệ thống thông tin; định kỳ hằng năm; và thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

c) Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền trong việc thường xuyên thực hiện giám sát an ninh mạng; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng; đề ra phương án ứng phó, khắc phục khẩn cấp;

d) Xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

đ) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong việc thực hiện kiểm tra an ninh mạng đột xuất.

2. Bộ Công an có trách nhiệm sau đây:

a) Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ;

b) Đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ;

c) Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng quốc gia, trừ hệ thống thông tin quân sự, hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước;

d) Thực hiện giám sát an ninh mạng; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng;

đ) Chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ; tham gia ứng phó, khắc phục sự cố khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng.

3. Bộ Quốc phòng chủ trì thẩm định, đánh giá, kiểm tra an ninh mạng đột xuẩt và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng do Bộ Quốc phòng quản lý.

4. Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin quan trọng quốc gia của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội; thẩm định, đánh giá, kiểm tra an ninh mạng đột xuất, giám sát an ninh mạng và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin cơ yếu; phối hợp với chủ quản hệ thống thông tin quan trọng quốc gia trong việc giám sát an ninh mạng theo quy định của pháp luật.

**MỤC 3:**

**PHÒNG NGỪA, XỬ LÝ HÀNH VI XÂM PHẠM AN NINH MẠNG**

# **Phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế**

1. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

2. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm:

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm:

a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

4. Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm:

a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác;

b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

5. Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

6. Chủ quản hệ thống thông tin có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng.

7. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng biện pháp quy định tại khoản 1 Điều 6 của Luật này để xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này.

8. Doanh nghiệp trong nướctrong và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin có trách nhiệm phối hợp với cơ quan chức năng xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này.

9. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật.

# **Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng**

1. Hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm:

a) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng;

c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư;

d) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;

đ) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

e) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

2. Chủ quản hệ thống thông tin có trách nhiệm sau đây:

a) Kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng;

b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này;

c) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

3. Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước.

4. Bộ Công an có trách nhiệm sau đây, trừ quy định tại khoản 5 và khoản 6 Điều này:

a) Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp;

b) Kiểm tra an ninh mạng đối với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng quốc gia;

c) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước;

d) Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng;

đ) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước theo quy định của pháp luật bảo vệ bí mật nhà nước và pháp luật cơ yếu; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao;

e) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng quốc gia;

g) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng quy định tại khoản 2 Điều 45 của Luật này.

5. Bộ Quốc phòng có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin quân sự.

6. Ban Cơ yếu Chính phủ có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ; có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

# **Phòng, chống xâm hại trẻ em trên không gian mạng**

1. Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng.

2. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; xây dựng, triển khai các hệ thống kỹ thuật hỗ trợ hoạt động ngăn chặn nội dung xâm hại trẻ em trên không gian mạng; điều phối các cơ quan, tổ chức, doanh nghiệp thực hiện ngăn chặn các nguồn phát tán thông tin xâm hại trẻ em trên không gian mạng; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

3. Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin mạng gây nguy hại cho trẻ em theo quy định của Luật này và pháp luật về trẻ em.

4. Cơ quan, tổ chức, cha mẹ, người giám hộ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em.

5. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

# **Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại**

1. Cơ quan, tổ chức, cá nhân có trách nhiệm thực hiện phòng ngừa, ngăn chặn phần mềm độc hại theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Chủ quản hệ thống thông tin quan trọng quốc gia triển khai hệ thống kỹ thuật nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời phần mềm độc hại.

3. Doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình và báo cáo cơ quan nhà nước có thẩm quyền theo quy định của pháp luật.

4. Doanh nghiệp cung cấp dịch vụ Internet có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền.

5. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh quốc gia.

# **Phòng, chống tấn công mạng**

1. Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm:

a) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của không gian mạng;

c) Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

d) Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính;

đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng gây hại mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật;

e) Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

2. Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi quy định tại các điểm a, b, c, d và e khoản 1 Điều này đối với hệ thống thông tin thuộc phạm vi quản lý.

3. Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

4. Trách nhiệm phòng, chống tấn công mạng được quy định như sau:

a) Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội trên phạm vi cả nước, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ.

# **Phòng, chống khủng bố mạng**

1. Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật này và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng.

2. Chủ quản hệ thống thông tin thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng.

3. Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng.

4. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp vô hiệu hóa nguồn khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra đối với hệ thống thông tin, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này.

5. Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự.

6. Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ.

# **Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng**

1. Tình huống nguy hiểm về an ninh mạng là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân, bao gồm:

a) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố;

b) Tấn công mạng vào hệ thống thông tin quan trọng quốc gia;

c) Tấn công mạng nhiều hệ thống thông tin trên quy mô lớn, cường độ cao;

d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia;

đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng được quy định như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng;

b) Doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

3. Chính phủ quy định chi tiết về phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

# **Đấu tranh bảo vệ an ninh mạng**

1. Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm:

a) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia;

b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng quốc gia;

c) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;

d) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

3. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.

# **Ngăn chặn xung đột thông tin trên mạng**

1. Ngăn chặn xung đột thông tin trên mạng là việc thực hiện các biện pháp công nghệ, kỹ thuật để giám sát, phát hiện, cảnh báo, xác định nguồn gốc, chặn lọc, khắc phục và loại trừ xung đột thông tin trên mạng.

2. Nội dung ngăn chặn xung đột thông tin trên mạng bao gồm:

a) Giám sát, phát hiện, cảnh báo, xung đột thông tin trên mạng;

b) Xác định nguồn gốc xung đột thông tin trên mạng;

c) Chặn lọc, khắc phục và loại trừ xung đột thông tin trên mạng;

d) Thông tin, tuyên truyền, giáo dục và hợp tác quốc tế về ngăn chặn xung đột thông tin trên mạng.

3. Tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm sau đây:

a) Ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;

b) Ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng;

c) Loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài.

4. Chính phủ quy định chi tiết về ngăn chặn xung đột thông tin trên mạng.

**CHƯƠNG III**

**PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO**

# **Phòng, chống tội phạm sử dụng không gian mạng trong lĩnh vực sản xuất, kinh doanh, thương mại và sở hữu trí tuệ**

1. Hành vi sử dụng không gian mạng xâm phạm trật tự quản lý kinh tế trong lĩnh vực sản xuất, kinh doanh, thương mại, bao gồm:

a) Vận chuyển trái phép hàng hóa, tiền tệ qua biên giới;

b) Kinh doanh, buôn bán hàng cấm, hàng giả;

c) Quảng cáo gian dối;

d) Lừa dối khách hàng;

đ) Vi phạm quy định trong hoạt động thương mại điện tử, kinh doanh dịch vụ vận tải và dịch vụ hỗ trợ cho vận tải;

e) Đăng tin quảng cáo, mua bán tài liệu, con dấu giả, hàng giả, hàng cấm, tem, nhãn, bao bì giả;

g) Kinh doanh hàng hóa nhập lậu, không rõ nguồn gốc, xuất xứ; hàng hóa lưu thông trong nước bị áp dụng biện pháp khẩn cấp; hàng hóa quá hạn sử dụng;

h) Xâm phạm quyền tác giả, quyền liên quan, quyền sở hữu công nghiệp;

i) Thiết lập, cung cấp dịch vụ hoặc hỗ trợ vận hành, kinh doanh, giao dịch, mua bán, tiếp thị trực tuyến cho các hình thức, sàn giao dịch, website, ứng dụng trái phép trên không gian mạng, gồm: Sàn thương mại điện tử; website, ứng dụng bán hàng, cung cấp dịch vụ thương mại điện tử; Sàn giao dịch dựa trên chỉ số các loại hàng hóa; Sàn giao dịch tài sản số, Kinh doanh theo phương thức đa cấp;

k) Các hành vi vi phạm pháp luật khác có sử dụng công nghệ cao trong lĩnh vực sản xuất, kinh doanh, thương mại.

2. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm thực hiện các biện pháp để đấu tranh, phòng, chống tội phạm sử dụng không gian mạng trong lĩnh vực sản xuất, kinh doanh, thương mại, sở hữu trí tuệ.

# **Phòng, chống tội phạm sử dụng không gian mạng trong lĩnh vực thuế, tài chính, ngân hàng, chứng khoán, bảo hiểm**

1. Hành vi sử dụng không gian mạng xâm phạm trật tự quản lý kinh tế trong lĩnh vực thuế, tài chính, ngân hàng, chứng khoán, bảo hiểm, bao gồm:

a) Thu thập, tàng trữ, trao đổi, mua bán, tặng cho, công khai hóa trái phép dữ liệu, thông tin tài khoản ngân hàng, thẻ ngân hàng, tài khoản ví điện tử, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và các loại tài khoản số khác;

b) Kinh doanh, cung cấp dịch vụ cho vay, huy động vốn trái phép trên không gian mạng, cho vay lãi nặng trong giao dịch dân sự;

c) Thiết lập, quảng cáo, cung cấp trái phép dịch vụ sàn cho vay ngang hàng, sàn giao dịch tiền ảo, chứng khoán, ngoại hối, trung gian thanh toán;

d) Rửa tiền, cung cấp trái phép dịch vụ rút tiền, chuyển tiền, nhận tiền hộ, chuyển đổi giá trị sang tiền từ thẻ trả trước dịch vụ viễn thông, thẻ trò chơi, tiền ảo, tài sản ảo và các loại tương tự;

đ) Tạo lập, đăng tin quảng cáo, mua bán ứng dụng ngân hàng giả, ứng dụng chứng khoán giả, tiền giả, công cụ chuyển nhượng giả hoặc các giấy tờ có giá giả khác;

e) Đưa thông tin giả, sai sự thật về lĩnh vực thuế, tài chính, ngân hàng, chứng khoán, bảo hiểm gây hoang mang dư luận xã hội, xâm phạm quyền lợi ích hợp pháp của nhà nước, tổ chức, cá nhân;

g) Làm giả tài liệu trong hồ sơ chào bán, niêm yết chứng khoán, cố ý công bố thông tin sai lệch hoặc che giấu thông tin trong hoạt động chứng khoán, sử dụng thông tin nội bộ để mua bán chứng khoán, thao túng thị trường chứng khoán;

i) Mua bán trái phép hóa đơn, chứng từ thu nộp ngân sách nhà nước;

k) Truy cập, sử dụng trái phép thông tin tài khoản ngân hàng, thẻ ngân hàng, tài khoản ví điện tử, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và các loại tài khoản số khác;

l) Lừa đảo chiếm đoạt tài sản trong thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh đoanh da cấp hoặc giao dịch chứng khoán qua không gian mạng nhằm nhiếm đoạt tài sản;

m) Sử dụng danh tính giả, thông tin của người khác, hồ sơ giả để thành lập doanh nghiệp, thiết lập, đăng ký tài khoản ngân hàng, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và tài khoản số khác;

n) Các hành vi vi phạm pháp luật khác có sử dụng công nghệ cao trong lĩnh vực thuế, tài chính, ngân hàng, chứng khoán, bảo hiểm, năng lượng, hải quan, chính phủ điện tử, dịch vụ hành chính công, thanh toán số, thanh toán điện tử, trung gian thanh toán; công nghệ tài chính.

2. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm thực hiện các biện pháp để đấu tranh, phòng, chống tội phạm sử dụng không gian mạng trong lĩnh vực thuế, tài chính, ngân hàng, chứng khoán, bảo hiểm.

# **Phòng, chống tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông**

1. Hành vi sử dụng không gian mạng xâm phạm trật tự công cộng trong lĩnh vực công nghệ thông tin, mạng viễn thông, bao gồm:

a) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật;

b) Phát tán chương trình tin học gây hại; nội dung vi phạm pháp luật hoặc vi phạm quy đinh về quảng cáo; cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử;

c) Đưa, sử dụng trái phép thông tin mạng máy tính, mạng viễn thông;

d) Xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của cơ quan, tổ chức, cá nhân;

đ) Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản;

e) Thiết lập, cung cấp, sử dụng trái phép dịch vụ viễn thông, Internet, dịch vụ ẩn danh, nặc danh;

g) Sử dụng trái phép tần số vô tuyến điện; gây nhiễu có hại, cản trở hoạt động bình thường của hệ thống thông tin vô tuyến điện, phương tiện điện tử;

h) Thu thập, tàng trữ, mua bán, trao đổi, công khai hóa trái phép tài khoản mạng xã hội, thông tin riêng hợp pháp của tổ chức, dữ liệu cá nhân;

i) Cho thuê, cho mượn, tẩy xóa, sửa chữa trái phép, mua bán căn cước, tài khoản định danh điện tử, chữ ký điện tử; tạo lập, làm giả danh tính; mua bán, sử dụng trái phép danh tính điện tử; thiết lập, cung cấp trái phép dịch vụ xác thực, định danh điện tử;

k) Các hành vi vi phạm pháp luật khác có sử dụng công nghệ cao trong trong lĩnh vực công nghệ thông tin, mạng viễn thông, bao gồm: sản xuất, vận chuyển, mua bán, lưu hành, thiết lập, kết nối, sử dụng, vận hành, giám sát, quản lý trái phép phần mềm, thiết bị, phương tiện điện tử, dịch vụ trực tuyến không hợp chuẩn, hợp quy vào hệ thống mạng máy tính, mạng viễn thông hoặc để thực hiện hành vi vi phạm pháp luật.

2. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm thực hiện các biện pháp để đấu tranh, phòng, chống tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông.

# **Phòng ngừa, xử lý hành vi sử dụng công nghệ cao xâm phạm trật tự xã hội**

1. Hành vi sử dụng công nghệ cao để vi phạm pháp luật, xâm phạm trật tự xã hội bao gồm:

a) Mua bán người, mô hoặc bộ phận cơ thể người;

b) Xúi giục người khác tự sát;

c) Chiếm đoạt tài sản;

d) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; sử dụng các phần mềm ứng dụng trí tuệ nhân tạo tạo ra các nội dung giả mạo nhằm thực hiện các hành vi vi phạm pháp luật;

đ) Mua bán trái phép vũ khí, vật liệu nổ, công cụ hỗ trợ, pháo nổ; ma túy, tiền chất ma túy, chất gây nghiện, chất hướng thần; văn bằng, chứng chỉ, giấy tờ giả; động vật hoang dã, nguy cấp, quý, hiếm; các hàng hóa, dịch vụ khác thuộc danh mục cấm theo quy định của pháp luật;

e) Tổ chức đánh bạc, đánh bạc; thiết lập, cung cấp trái phép trò chơi trực tuyến;

g) Môi giới mại dâm; truyền bá văn hóa phẩm đồi trụy; Lạm dụng tình dục trẻ em; quấy rối tình dục;

h) Tổ chức, môi giới cho người khác xuất cảnh, nhập cảnh hoặc ở lại Việt Nam trái phép;

i) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

k) Hành vi khác sử dụng công nghệ cao vi phạm pháp luật, xâm phạm trật tự xã hội.

2. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm thực hiện các biện pháp để đấu tranh, phòng, chống tội phạm âm phạm trật tự xã hội.

# **Thẩm quyền của lực lượng chuyên trách bảo vệ an ninh mạng trong phòng, chống tội phạm sử dụng công nghệ cao.**

1. Trong quá trình thực hiện công tác phòng, chống tội phạm sử dụng công nghệ cao, Lực lượng chuyên trách bảo vệ an ninh mạng được quyền:

a) Thực hiện biện pháp điều tra tố tụng đặc biệt theo quy định Bộ luật TTHS và các biện pháp nghiệp vụ khác theo quy định của pháp luật.

b) Kiểm tra phương tiện điện tử, giám sát, phát hiện, thu thập, phục hồi và phân tích, giám định thông tin, tài liệu, dữ liệu điện tử phục vụ phát hiện, điều tra, xử lý tội phạm và các vi phạm pháp luật có sử dụng công nghệ cao.

c) Yêu cầu nhà cung cấp dịch vụ, tổ chức, cá nhân sử dụng dịch vụ cung cấp thông tin, tài liệu, đồ vật, phương tiện điện tử, dữ liệu điện tử; bố trí mặt bằng, cổng kết nối, các điều kiện kỹ thuật cần thiết để lực lượng chuyên trách triển khai các phương tiện, biện pháp kỹ thuật kiểm tra, giám sát, thu thập dữ liệu điện tử phục vụ công tác phòng ngừa, phát hiện, điều tra, xử lý tội phạm và vi phạm pháp luật có sử dụng công nghệ cao;.

d) Yêu cầu nhà cung cấp dịch vụ đóng tài khoản số, phong tỏa, mở phong tỏa tài khoản số, tạm dừng giao dịch, hoạt động của tài khoản số, định danh, xác thực lại tài khoản số phục vụ công tác phòng ngừa, phát hiện, điều tra, xử lý tội phạm và vi phạm pháp luật có sử dụng công nghệ cao;

đ) Trực tiếp hoặc phối hợp với cơ quan nhà nước có thẩm quyền yêu cầu nhà cung cấp dịch vụ ngăn chặn, tạm đình chỉ, đình chỉ hoạt động của trang thông tin điện tử, hệ thống thông tin, phương tiện điện tử, cung cấp dịch vụ, thu hồi giấy phép hoạt động;

e) Thu giữ, tạm giữ đồ vật, tài liệu, phương tiện điện tử, dữ liệu điện tử, tài sản số liên quan đến hành vi vi phạm pháp luật có sử dụng công nghệ cao.

g) Cảnh báo, yêu cầu nhà cung cấp dịch vụ cảnh báo thông tin về an ninh mạng, tổ chức, cá nhân, tài khoản ngân hàng, ví điện tử, tài khoản chứng khoán và các loại tài khoản số khác nghi vấn liên quan đến hoạt động vi phạm pháp luật phục vụ công tác phòng ngừa, ngăn chặn tội phạm và các hành vi vi phạm pháp luật khác có sử dụng công nghệ cao.

h) Thực hiện các nhiệm vụ, quyền hạn khác theo quy định của pháp luật.

2. Chính phủ quy định chi tiết điểm a khoản 1 Điều này.

# **Trách nhiệm của nhà cung cấp dịch vụ, tổ chức, cá nhân sử dụng dịch vụ đấu tranh phòng, chống tội phạm sử dụng công nghệ cao**

1. Nhà cung cấp dịch vụ có trách nhiệm:

a) Định danh, xác thực tổ chức, cá nhân sử dụng dịch vụ trước và trong quá trình cung cấp dịch vụ; có giải pháp xác định, ngăn chặn tình trạng sử dụng dịch vụ, tài khoản số không chính chủ; giữ bí mật thông tin, tài liệu về tổ chức, cá nhân sử dụng dịch vụ;

b) Chấp hành quy định của pháp luật về bảo mật, thời hạn bảo quản, lưu trữ, cung cấp thông tin, dữ liệu điện tử phục vụ công tác phòng, chống tội phạm sử dụng công nghệ cao;

c) Có trách nhiệm phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thực hiện nhiệm vụ;

d) Thực hiện theo hướng dẫn của Bộ Công an về việc kết nối, tiếp nhận, trả lời văn bản điện tử phục vụ công tác bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao;

đ) Cung cấp thông tin, tài liệu đầy đủ, chính xác, đúng thời hạn, đảm bảo bí mật cho cơ quan có thẩm quyền theo quy định của luật này và quy định của luật khác có liên quan;

e) Thực hiện ngay các biện pháp cần thiết theo hướng dẫn của cơ quan có thẩm quyền khi nhận được thông tin cảnh báo về an ninh mạng và tội phạm sử dụng công nghệ cao;

g) Chịu trách nhiệm về những thiệt hại phát sinh trong trường hợp không thực hiện theo hướng dẫn của cơ quan có thẩm quyền;

h) Chủ quản hệ thống thông tin có trách nhiệm báo cáo lực lượng chuyên trách về an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao trong thời hạn 24 giờ kể từ khi phát hiện hành vi tấn công mạng.

2. Trách nhiệm của tổ chức, cá nhân sử dụng dịch vụ

a) Có trách nhiệm bảo mật thông tin đăng ký, mở, quản lý, sử dụng tài khoản số của mình; trường hợp tài khoản số được sử dụng để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ vi phạm, chủ tài khoản bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường thiệt hại theo quy định pháp luật;

b) Cung cấp thông tin, tài liệu cho cơ quan có thẩm quyền, nhà cung cấp dịch vụ trung thực, đầy đủ theo quy định pháp luật.

**Chương IV**

**TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN NINH MẠNG**

# **Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng**

1. Tiêu chuẩn an ninh mạng gồm tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn nước ngoài, tiêu chuẩn quốc gia và tiêu chuẩn cơ sở đối với sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng được công bố, thừa nhận áp dụng tại Việt Nam.

2. Quy chuẩn kỹ thuật an ninh mạng gồm quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng được xây dựng, ban hành và áp dụng tại Việt Nam.

# **Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng**

1. Chứng nhận hợp quy về an ninh mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng phù hợp với quy chuẩn kỹ thuật an ninh mạng.

2. Công bố hợp quy về an ninh mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng với quy chuẩn kỹ thuật an ninh mạng.

3. Chứng nhận hợp chuẩn về an ninh mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng phù hợp với tiêu chuẩn an ninh mạng.

4. Công bố hợp chuẩn về an ninh mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng với tiêu chuẩn an ninh mạng.

5. Bộ Khoa học và Công nghệ chủ trì, phối hợp với cơ quan có liên quan tổ chức thẩm định và công bố tiêu chuẩn quốc gia về an ninh mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

6. Bộ Công an có trách nhiệm sau đây:

a) Xây dựng dự thảo tiêu chuẩn quốc gia an ninh mạng, trừ tiêu chuẩn quốc gia quy định tại khoản 7 Điều này;

b) Ban hành quy chuẩn kỹ thuật quốc gia an ninh mạng, trừ quy chuẩn quốc gia quy định tại khoản 7 Điều này; quy định về đánh giá hợp quy về an ninh mạng;

c) Quản lý chất lượng sản phẩm, dịch vụ an ninh mạng, trừ sản phẩm, dịch vụ mật mã dân sự;

d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng, trừ tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự.

7. Ban Cơ yếu Chính phủcó trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự.

# **Đánh giá hợp chuẩn, hợp quy về an ninh mạng**

1. Việc đánh giá hợp chuẩn, hợp quy về an ninh mạng được thực hiện trong các trường hợp sau đây:

a) Trước khi tổ chức, cá nhân đưa sản phẩm an ninh mạng vào lưu thông trên thị trường phải thực hiện chứng nhận hợp quy hoặc công bố hợp quy và sử dụng dấu hợp quy;

b) Phục vụ hoạt động quản lý nhà nước về an ninh mạng.

2. Việc đánh giá hợp chuẩn, hợp quy về an ninh mạng phục vụ hệ thống thông tin quan trọng quốc gia và phục vụ hoạt động quản lý nhà nước về an ninh mạng được thực hiện tại tổ chức chứng nhận hợp chuẩn, hợp quy.

3. Tổ chức chứng nhận hợp chuẩn, hợp quy về an ninh mạng là tổ chức được Bộ Công an chỉ định, thừa nhận hoặc công nhận đủ năng lực thực hiện hoạt động chứng nhận hợp chuẩn, hợp quy về an ninh mạng. Chính phủ quy định cụ thể về Tổ chức chứng nhân hợp chuẩn, hợp quy về an ninh mạng.

4. Nhãn an ninh mạng là chứng nhận do Bộ Công an cấp cho sản phẩm, dịch vụ an ninh mạng hợp chuẩn, hợp quy khi doanh nghiệp, cá nhân có yêu cầu. Chính phủ quy định cụ thể về nhãn an ninh mạng.

5. Việc thừa nhận kết quả đánh giá hợp chuẩn, hợp quy về an ninh mạng giữa Việt Nam với quốc gia, vùng lãnh thổ khác, giữa tổ chức chứng nhận sự phù hợp của Việt Nam với tổ chức chứng nhận sự phù hợp của quốc gia, vùng lãnh thổ khác được thực hiện theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

**Chương V**

**SẢN PHẨM, DỊCH VỤ AN NINH MẠNG**

**MỤC 1:**

**CẤP GIẤY PHÉP KINH DOANH SẢN PHẨM, DỊCH VỤ AN NINH MẠNG**

# **Sản phẩm, dịch vụ an ninh mạng**

1. Dịch vụ an ninh mạng gồm:

a) Dịch vụ kiểm tra, đánh giá an ninh mạng;

b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự;

c) Dịch vụ mật mã dân sự;

d) Dịch vụ chứng thực chữ ký điện tử;

đ) Dịch vụ tư vấn an ninh mạng;

e) Dịch vụ giám sát an ninh mạng;

g) Dịch vụ ứng cứu sự cố an ninh mạng;

h) Dịch vụ khôi phục dữ liệu;

i) Dịch vụ phòng ngừa, chống tấn công mạng;

k) Dịch vụ an ninh mạng khác.

2. Sản phẩm an ninh mạng gồm:

a) Sản phẩm mật mã dân sự;

b) Sản phẩm kiểm tra, đánh giá an ninh mạng;

c) Sản phẩm giám sát an ninh mạng;

d) Sản phẩm chống tấn công, xâm nhập;

đ) Sản phẩm an ninh mạng khác.

3. Chính phủ quy định chi tiết danh mục sản phẩm, dịch vụ an ninh mạng quy định tại khoản 1, 2 Điều này.

# **Điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng**

1. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng, trừ sản phẩm, dịch vụ quy định tại các điểm a, b, c, d khoản 1 và điểm a khoản 2 Điều 38 của Luật này, khi đáp ứng đủ các điều kiện sau đây:

a) Phù hợp với chiến lược, quy hoạch, kế hoạch phát triển an ninh mạng quốc gia;

b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ an ninh mạng;

c) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng được yêu cầu chuyên môn về an ninh mạng;

d) Có phương án kinh doanh phù hợp.

2. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ kiểm tra, đánh giá an ninh mạng khi đáp ứng đủ các điều kiện sau đây:

a) Các điều kiện quy định tại khoản 1 Điều này;

b) Là doanh nghiệp được thành lập và hoạt động hợp pháp trên lãnh thổ Việt Nam, trừ doanh nghiệp có vốn đầu tư nước ngoài;

c) Người đại diện theo pháp luật, đội ngũ quản lý, điều hành, kỹ thuật là công dân Việt Nam thường trú tại Việt Nam;

d) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật;

đ) Có phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ;

e) Đội ngũ quản lý, điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về kiểm tra, đánh giá an ninh mạng.

3. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ bảo mật thông tin không sử dụng mật mã dân sự khi đáp ứng đủ các điều kiện sau đây:

a) Các điều kiện quy định tại các điểm a, b, c, d và đ khoản 2 Điều này;

b) Đội ngũ quản lý điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về bảo mật thông tin.

4. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ mật mã dân sự khi đáp ứng đủ các yêu cầu sau đây:

a) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng yêu cầu chuyên môn về bảo mật, an ninh mạng;

b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ mật mã dân sự;

c) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật;

d) Có phương án bảo mật và an ninh mạng trong quá trình quản lý và cung cấp sản phẩm, dịch vụ mật mã dân sự;

đ) Có phương án kinh doanh phù hợp;

e) Sản phẩm mật mã dân sự phải được kiểm định, chứng nhận hợp quy trước khi lưu thông trên thị trường.

5. Chính phủ quy định chi tiết về kinh doanh sản phẩm, dịch vụ an ninh mạng.

# **Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng**

1. Quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, báo cáo Bộ Công an về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng khi có yêu cầu.

2. Lập, lưu giữ và bảo mật thông tin của khách hàng.

3. Từ chối cung cấp sản phẩm, dịch vụ an ninh mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an ninh mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp.

4. Tạm ngừng hoặc ngừng cung cấp sản phẩm, dịch vụ an ninh mạng để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của cơ quan nhà nước có thẩm quyền.

5. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nghiệp vụ khi có yêu cầu.

**MỤC 2:**

**QUẢN LÝ XUẤT KHẨU, NHẬP KHẨU SẢN PHẨM AN NINH MẠNG**

# **Nguyên tắc quản lý xuất khẩu, nhập khẩu sản phẩm an ninh mạng**

1. Việc quản lý xuất khẩu, nhập khẩu đối với sản phẩm an ninh mạng được thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Việc xuất khẩu, nhập khẩu sản phẩm an ninh mạng của cơ quan, tổ chức, cá nhân được hưởng quyền ưu đãi, miễn trừ ngoại giao thực hiện theo quy định của pháp luật về hải quan, pháp luật về ưu đãi, miễn trừ dành cho cơ quan đại diện ngoại giao, cơ quan lãnh sự của nước ngoài và cơ quan đại diện của tổ chức quốc tế liên Chính phủ tại Việt Nam.

3. Trong trường hợp Việt Nam chưa có quy chuẩn kỹ thuật an ninh mạng tương ứng đối với sản phẩm an ninh mạng nhập khẩu thì áp dụng theo thỏa thuận quốc tế, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

# **Sản phẩm xuất khẩu, nhập khẩu theo giấy phép trong lĩnh vực an ninh mạng**

1. Khi xuất khẩu, nhập khẩu sản phẩm an ninh mạng thuộc Danh mục sản phẩm an ninh mạng xuất khẩu, nhập khẩu theo giấy phép do Chính phủ quy định, doanh nghiệp phải có Giấy phép xuất khẩu, nhập khẩu sản phẩm an ninh mạng do cơ quan nhà nước có thẩm quyền cấp.

2. Tổ chức, doanh nghiệp xuất khẩu, nhập khẩu sản phẩm an ninh mạng phải thực hiện chứng nhận, công bố hợp quy trước khi xuất, nhập khẩu theo quy định tại Điều 39 của Luật này.

3. Tổ chức, doanh nghiệp được cấp Giấy phép xuất khẩu, nhập khẩu sản phẩm an ninh mạng khi đáp ứng đủ các điều kiện sau đây:

a) Có Giấy phép kinh doanh sản phẩm an ninh mạng;

b) Sản phẩm an ninh mạng phải thực hiện chứng nhận, công bố hợp quy theo quy định tại Điều 41 của Luật này;

c) Đối tượng và mục đích sử dụng sản phẩm an ninh mạng không gây phương hại đến quốc phòng, an ninh quốc gia và trật tự, an toàn xã hội.

4. Chính phủ quy định chi tiết về trình tự, thủ tục, hồ sơ cấp Giấy phép xuất khẩu, nhập khẩu sản phẩm an ninh mạng theo giấy phép.

**Chương VI**

**ĐIỀU KIỆN BẢO ĐẢM AN NINH MẠNG**

# **Nghiên cứu, phát triển an ninh mạng**

1. Nội dung nghiên cứu, phát triển an ninh mạng bao gồm:

a) Xây dựng hệ thống phần mềm, trang thiết bị bảo vệ an ninh mạng;

b) Phương pháp thẩm định phần mềm, trang thiết bị bảo vệ an ninh mạng đạt chuẩn và hạn chế tồn tại điểm yếu, lỗ hổng bảo mật, phần mềm độc hại;

c) Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng;

d) Phương pháp bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; khả năng bảo mật khi truyền đưa thông tin trên không gian mạng;

đ) Xác định nguồn gốc của thông tin được truyền đưa trên không gian mạng;

e) Giải quyết nguy cơ đe dọa an ninh mạng;

g) Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng;

h) Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng;

i) Dự báo an ninh mạng;

k) Nghiên cứu thực tiễn, phát triển lý luận an ninh mạng.

2. Cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.

# **Nâng cao năng lực tự chủ về an ninh mạng**

1. Nhà nước khuyến khích, tạo điều kiện để cơ quan, tổ chức, cá nhân nâng cao năng lực tự chủ về an ninh mạng và nâng cao khả năng sản xuất, kiểm tra, đánh giá, kiểm định thiết bị số, dịch vụ mạng, ứng dụng mạng.

2. Chính phủ thực hiện các biện pháp sau đây để nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân:

a) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng;

b) Thúc đẩy ứng dụng công nghệ mới, công nghệ tiên tiến liên quan đến an ninh mạng;

c) Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng;

d) Tăng cường môi trường kinh doanh, cải thiện điều kiện cạnh tranh hỗ trợ doanh nghiệp nghiên cứu, sản xuất sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng.

# **Lực lượng bảo vệ an ninh mạng**

1. Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng.

2. Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng quốc gia.

3. Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

4. Chính phủ quy định chi tiết về lực lượng bảo vệ an ninh mạng.

# **Bảo đảm nguồn nhân lực bảo vệ an ninh mạng**

1. Công dân Việt Nam có kiến thức về an ninh mạng, công nghệ thông tin là nguồn lực cơ bản, chủ yếu bảo vệ an ninh mạng.

2. Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng.

3. Khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc nguy cơ đe dọa an ninh mạng, cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng.

Thẩm quyền, trách nhiệm, trình tự, thủ tục huy động nhân lực bảo vệ an ninh mạng được thực hiện theo quy định của Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và quy định khác của pháp luật có liên quan.

# **Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng**

1. Công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng.

2. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao.

3. Ưu tiên phát triển cơ sở đào tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà nước và khu vực tư nhân, trong nước và nước ngoài.

# **Giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng**

1. Nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường, chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh.

2. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan tổ chức huấn luyện, bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng.

Bộ Quốc phòng, Ban Cơ yếu Chính phủ tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý.

# **Phổ biến kiến thức về an ninh mạng**

1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng.

2. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức.

3. Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.

# **Kinh phí bảo vệ an ninh mạng**

1. Kinh phí bảo vệ an ninh mạng của cơ quan nhà nước, tổ chức chính trị do ngân sách nhà nước bảo đảm, được bố trí trong dự toán ngân sách nhà nước hằng năm. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật về ngân sách nhà nước.

2. Kinh phí bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan, tổ chức ngoài quy định tại khoản 1 Điều này do cơ quan, tổ chức tự bảo đảm.

# **Văn bằng, chứng chỉ đào tạo về an ninh mạng**

1. Cơ sở giáo dục đại học, cơ sở giáo dục nghề nghiệp trong phạm vi nhiệm vụ, quyền hạn của mình cấp văn bằng, chứng chỉ đào tạo về an ninh mạng.

2. Bộ Giáo dục và Đào tạo chủ trì, phối hợp với Bộ Công an, bộ, ngành có liên quan công nhận văn bằng giáo dục đại học về an ninh mạng do tổ chức nước ngoài cấp.

3. Bộ Giáo dục và Đào tạo chủ trì, phối hợp với Bộ Công an, bộ, ngành có liên quan công nhận văn bằng, chứng chỉ giáo dục nghề nghiệp về an ninh mạng do tổ chức nước ngoài cấp.

**CHƯƠNG VII**

**QUẢN LÝ NHÀ NƯỚC VỀ AN NINH MẠNG**

# **Nội dung quản lý nhà nước về an ninh mạng**

1. Xây dựng chủ trương, chính sách, chiến lược, quy hoạch, kế hoạch, chương trình trong lĩnh vực an ninh mạng.

2. Ban hành và tổ chức thực hiện văn bản quy phạm pháp luật về an ninh mạng; xây dựng, công bố tiêu chuẩn quốc gia, ban hành quy chuẩn kỹ thuật về an ninh mạng.

3. Quản lý nhà nước về mật mã dân sự.

4. Quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy về an ninh mạng.

5. Quản lý công tác giám sát an ninh mạng.

6. Thẩm định về an ninh mạng trong hồ sơ thiết kế hệ thống thông tin.

7. Tuyên truyền, phổ biến pháp luật về an ninh mạng.

8. Quản lý hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng.

9. Tổ chức nghiên cứu, ứng dụng khoa học và công nghệ về an ninh mạng; phát triển nguồn nhân lực an ninh mạng; đào tạo về an ninh mạng.

10. Phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, tội phạm sử dụng công nghệ cao.

11. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo, xử lý vi phạm pháp luật về an ninh mạng.

12. Hợp tác quốc tế về an ninh mạng.

# **Trách nhiệm quản lý nhà nước về an ninh mạng**

1. Chính phủ thống nhất quản lý nhà nước về an ninh mạng.

2. Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện thống nhất quản lý nhà nước về an ninh mạng trên phạm vi toàn quốc, trừ quy định tại khoản 3 Điều này.

3. Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng thuộc phạm vi quản lý.

Ban Cơ yếu Chính phủ chịu trách nhiệm trước Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự và an ninh mạng thuộc phạm vi quản lý theo quy định của pháp luật về cơ yếu.

5. Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình thực hiện công tác bảo vệ an ninh mạng; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng;

6. Ủy ban nhân dân cấp tỉnh thực hiện công tác bảo vệ an ninh mạng và quản lý nhà nước về dữ liệu tại địa phương.

# **Trách nhiệm của chủ quản hệ thống thông tin**

1. Chủ quản hệ thống thông tin có trách nhiệm thực hiện bảo vệ hệ thống thông tin theo quy định tại Luật này.

2. Chủ quản hệ thống thông tin sử dụng ngân sách nhà nước thực hiện trách nhiệm quy định tại khoản 1 Điều này và có trách nhiệm sau đây:

a) Có phương án bảo đảm an ninh mạng được cơ quan nhà nước có thẩm quyền thẩm định khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin;

b) Chỉ định cá nhân, bộ phận phụ trách về an ninh mạng.

# **Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng**

1. Doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm sau đây:

a) Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa;

b) Xây dựng phương án, giải pháp phản ứng nhanh với sự cố an ninh mạng, xử lý ngay điểm yếu, lỗ hổng bảo mật, mã độc, tấn công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này;

c) Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này;

d) Phối hợp lực lượng chuyên trách bảo vệ an ninh mạng trong bảo vệ an ninh mạng.

2. Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm thực hiện quy định tại khoản 1 Điều này, khoản 2 và khoản 3 Điều 12 của Luật này.

# **Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng**

1.Tuân thủ quy định của pháp luật về an ninh mạng.

2. Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng.

3. Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

**Chương VIII**

**ĐIỀU KHOẢN THI HÀNH**

# **Điều khoản chuyển tiếp**

1. Các cơ quan, tổ chức, cá nhân có trách nhiệm hoàn thành việc chuyển đổi các nội dung liên quan từ Luật An toàn thông tin mạng năm 2015 sang tuân thủ theo quy định của Luật An ninh mạng năm 2025 trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

Trong thời gian chưa hoàn thành việc chuyển đổi, các cơ quan, tổ chức, cá nhân tiếp tục áp dụng các quy định của Luật An toàn thông tin mạng không trái với quy định của Luật này.

2. Đối với các hồ sơ hệ thống thông tin đã có Quyết định công nhận cấp độ trước khi Luật này có hiệu lực thì không cần hoàn thiện hồ sơ theo quy định cấp độ mới, nhưng áp dụng các điều kiện, tiêu chuẩn, biện pháp bảo vệ tương ướng với quy định cấp độ mới trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

3. Đối với hệ thống thông tin quan trọng về an ninh quốc gia đã đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành:

a) Chủ quản hệ thống thông tin có trách nhiệm rà soát, đánh giá và thực hiện các biện pháp bảo đảm an ninh mạng theo quy định của Luật này;

b) Trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành, chủ quản hệ thống thông tin phải hoàn thành việc đánh giá điều kiện an ninh mạng và thẩm định an ninh mạng theo quy định của Luật này.

4. Các phương án, quy trình, thủ tục bảo đảm an toàn thông tin được ban hành theo Luật An toàn thông tin mạng năm 2015 phải được rà soát, điều chỉnh, bổ sung cho phù hợp với các quy định của Luật này trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

5. Các sản phẩm, dịch vụ, giải pháp, phương tiện kỹ thuật bảo đảm an toàn thông tin mạng đã được đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành, nếu không đáp ứng các điều kiện an ninh mạng theo quy định của Luật này thì phải được thay thế hoặc nâng cấp trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

6. Chính phủ quy định chi tiết việc thực hiện các điều khoản chuyển tiếp quy định tại Điều này.

# **Hiệu lực thi hành**

1. Luật này có hiệu lực th hành từ ngày 01 tháng 01 năm 2026.

2. Luật này thay thế Luật An toàn thông tin năm 2015, Luật An ninh mạng năm 2018.

*Luật này được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XV, kỳ họp thứ 10 thông qua ngày tháng năm 2025.*

**CHỦ TỊCH QUỐC HỘI**