MỤC LỤC

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

LUẬT
AN NINH MẠNG

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam đã được sửa đổi, bổ sung một số điều theo Nghị quyết số 203/2025/QH15;

Quốc hội ban hành Luật An ninh mạng.

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Luật này quy định về hoạt động bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội, bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng; bảo đảm an ninh thông tin, an ninh dữ liệu, an toàn hệ thống thông tin; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

Điều 2. Đối tượng áp dụng

Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng tại Việt Nam.

Điều 3. Giải thích từ ngữ

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

1. An ninh mạng là sự bảo đảm hoạt động trên không gian mạng 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; bảo đảm an ninh dữ liệu, an ninh thông tin mạng và bảo vệ hệ thống thông tin

2. An ninh thông tin mạng là bảo đảm thông tin trên không gian mạng không bị sử dụng, tiết lộ, sửa đổi hoặc xóa bỏ trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin và không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

3. An ninh dữ liệu là sự bảo đảm hoạt động thu thập, cập nhật, điều chỉnh, xử lý dữ liệu phục vụ chuyển đổi số quốc gia và phát triển kinh tế số gắn với bảo đảm quốc phòng, an ninh, đối ngoại, cơ yếu.

4. Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

5. 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.

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

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

8. 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.

9. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.

10. 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.

11. 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.

12. Phần cứng độc hại là các bộ phận vật lý của hệ thống máy tính, hệ thống thông tin, được tạo ra có chủ đích, nằm ngoài thiết kế và quy cách thiết bị tiêu chuẩn, có thể được điều khiển hoặc thực hiện tính năng can thiệp vào phần mềm, phần cứng hệ thống, gây ra tác động bất bình thường cho một phần hay toàn bộ hệ thống máy tính, hệ thống thông tin, hoặc đánh cắp thông tin, dữ liệu trái phép lưu trữ trong hệ thống máy tính, hệ thống thông tin, hoặc gây ngừng trệ, tê liệt, phá hoại hệ thống tùy theo mục đích thiết kế.

13. 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.

14. Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự.

15. 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 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.

16. 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.

17. Gián điệp mạng là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác nhằm chiếm đoạt, thu thập trái phép tài liệu, thông tin bí mật, tài nguyên thông tin của cơ quan, tổ chức Nhà nước hoặc nhằm mục đích gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

18. Nguy cơ đe dọa an ninh mạng là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

19. 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.

20. 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.

21. 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.

22. Tài khoản số là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.

23. 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.

24. Sản phẩm an ninh mạng là phần cứng, phần mềm có chức năng bảo vệ an ninh mạng, an ninh thông tin, an ninh dữ liệu, thông tin, hệ thống thông tin, cơ sở hạ tầng công nghệ thông tin.

25. Dịch vụ an ninh mạng là dịch vụ được cung cấp để bảo vệ an ninh mạng, an ninh thông tin, an ninh dữ liệu, thông tin, hệ thống thông tin, cơ sở hạ tầng công nghệ thông tin.

26. Hệ thống thông tin cơ yếu là các hệ thống thông tin thuộc Ban cơ yếu Chính phủ và hệ thống thông tin có sử dụng các giải pháp, sản phẩm mật mã của ngành Cơ yếu Việt Nam để phục vụ hoạt động chuyên môn nghiệp vụ cơ yếu do tổ chức cơ yếu trực tiếp quản lý, vận hành.

Điều 4. Chính sách của Nhà nước về an ninh mạng

1. Ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, cơ yếu, 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, bảo đảm nguồn nhân lực trình độ cao cho 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; có cơ chế đặc thù, chính sách ưu đãi để huy động, thu hút và sử dụng nhân tài trong lĩnh vực 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. Khuyến khích các cơ quan, tổ chức, cá nhân sử dụng sản phẩm, dịch vụ công nghiệp an ninh mạng của Việt Nam.

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

Điều 5. Nguyên tắc bảo vệ an ninh mạng

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng.

2. Đặt dưới sự lãnh đạo tuyệt đối, trực tiếp 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 về an ninh quốc gia, bảo vệ an ninh dữ liệu 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 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.

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

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

Điều 6. Biện pháp bảo vệ an ninh mạng

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

a) Thẩm định an ninh mạng;

b) Đánh giá điều kiện an ninh mạng;

c) Kiểm tra an ninh mạng;

d) Giám sát an ninh mạng;

đ) Ứng phó, khắc phục sự cố an ninh mạng;

e) Đấu tranh bảo vệ an ninh mạng;

g) Sử dụng mật mã để bảo vệ thông tin mạng;

h) Sử dụng giải pháp kỹ thuật để bảo vệ an ninh dữ liệu, an ninh thông tin, hệ thống thông tin; ngăn chặn thông tin vi phạm pháp luật;

i) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

k) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật, tin giả 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;

l) Thu thập dữ liệu điện tử liên quan đến hoạt động 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;

m) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật;

n) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự;

o) Biện pháp khác theo quy định của pháp luật về bảo vệ an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

2. Chính phủ quy định chi tiết về nội dung, trình tự, thủ tục, thẩm quyền áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm n và điểm o khoản 1 Điều này.

Điều 7. Bảo vệ không gian mạng quốc gia

Nhà nước áp dụng các biện pháp để bảo vệ 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.

Điều 8. 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, tham gia 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.

3. Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.

Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vi quản lý.

Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng.

Trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều Bộ, ngành do Chính phủ quyết định.

4. Hoạt động hợp tác quốc tế về an ninh mạng của Bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.

Điều 9. Các hành vi bị nghiêm cấm về an ninh mạng

1. Sử dụng không gian mạng để đăng tải, phát tán thông tin có nội dung:

a) Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; 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; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

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

c) Bịa đặt, vu khống, vu cáo sai sự thật, xúc phạm danh dự, uy tín, nhân phẩm của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

d) 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; 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; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, kinh doanh đa cấp, chứng khoán.

2. 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) Kích động, 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; 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;

c) 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; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; 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; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

đ) Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

e) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức Nhà nước;

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

h) Hướng dẫn, xúi giục, lôi kéo, kích động người khác phạm tội hoặc thực hiện hành vi vi phạm pháp luật;

i) Thực hiện hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

3. Thực hiện tấn công mạng; khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin.

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 mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán thư rác, tin nhắn rác, cuộc gọi rác, chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển 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.

Điều 10. Xử lý vi phạm pháp luật về an ninh mạng

Người nào 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
BẢO VỆ AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN VÀ HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 11. 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 để áp dụng biện pháp bảo vệ tương ứng, phù hợp theo từng cấp độ tăng dần từ 1 đến 5.

2. Hệ thống thông tin được phân loại theo cấp độ như sau:

a) Cấp độ 1 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại 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 sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

c) Cấp độ 3 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;

d) Cấp độ 4 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;

đ) Cấp độ 5 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới chủ quyền, lợi ích, quốc phòng, an ninh 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; các biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin và trách nhiệm, nghĩa vụ bảo đảm an ninh mạng theo từng cấp độ của hệ thống thông tin.

Điều 12. Nhiệm vụ bảo vệ hệ thống thông tin

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

a) Xác định cấp độ an ninh mạng của hệ thống thông tin và hệ thống thông tin quan trọng về an ninh quốc gia;

b) Đánh giá và quản lý rủi ro an ninh mạng hệ thống thông tin;

c) Đôn đốc, giám sát, kiểm tra công tác bảo vệ an ninh mạng hệ thống thông tin;

d) Tổ chức triển khai các biện pháp bảo vệ an ninh mạng hệ thống thông tin;

đ) Thực hiện chế độ báo cáo theo quy định;

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

2. Chủ quản hệ thống thông tin thuộc Cấp độ 1 và Cấp độ 2 tự chịu trách nhiệm thực hiện các nội dung quy định tại Khoản 1 Điều này.

3. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4, Cấp độ 5 phải thực hiện đầy đủ các nội dung nhiệm vụ quy định tại Khoản 1 Điều này.

4. Chính phủ quy định chi tiết khoản 1 Điều này.

Điều 13. Biện pháp bảo vệ hệ thống thông tin

1. Các biện pháp bảo vệ đối với hệ thống thông tin, bao gồm:

a) 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;

b) Thẩm định an ninh mạng đối với hồ sơ, thiết kế của hệ thống thông tin;

c) Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin;

d) Áp dụng biện pháp quản lý theo tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng, nghiên cứu xây dựng hệ thống tường lửa quốc gia để phòng, chống nguy cơ, khắc phục sự cố an ninh mạng;

đ) Tổ chức triển khai các biện pháp lưu trữ, sao lưu bảo vệ an ninh thông tin mạng và an ninh của các thành tố cấu thành hệ thống thông tin;

e) 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;

g) Thực hiện giám sát an ninh mạng;

h) Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin.

2. Chủ quản hệ thống thông tin thuộc Cấp độ 1 và Cấp độ 2 theo nhu cầu và khả năng đáp ứng thực tế lựa chọn áp dụng đầy đủ hoặc một số biện pháp quy định tại khoản 1 Điều này.

3. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4, Cấp độ 5 phải áp dụng đầy đủ các biện pháp quy định tại khoản 1 Điều này.

4. Chính phủ quy định chi tiết khoản 1 Điều này.

Điều 14. Hệ thống thông tin quan trọng về an ninh quốc gia

1. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin thuộc Cấp độ 5 hoặc hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4 khi đáp ứng một số tiêu chí nhất định.

2. Danh mục hệ thống thông tin quan trọng về an ninh quốc gia là danh sách hệ thống thông tin quan trọng về an ninh quốc gia được xác lập, ban hành và áp dụng biện pháp bảo vệ tương xứng nhằm bảo đảm 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.

3. Hệ thống thông tin quan trọng về an ninh quốc gia phải 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.

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

5. Chính phủ quy định chi tiết khoản 1 và khoản 3 Điều này.

Điều 15. Trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

a) Thực hiện quy định tại khoản 1 Điều 12 và khoản 1 Điều 13 Luật này;

b) Khi thiết lập, mở rộng và nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia phải thực hiện kiểm định an ninh mạng trước khi đi vào vận hành, khai thác; định kỳ hằng năm, tự kiểm tra, đánh giá an ninh mạng hệ thống thông tin quan trọng về an ninh quốc gia 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 đối với các hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu do Bộ Quốc phòng và Ban Cơ yếu Chính phủ quản lý theo quy định của pháp luật:

a) Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

b) Đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

c) Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia;

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 đối với hệ thống thông tin quan trọng về an ninh quốc gia;

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 về an ninh quốc gia, 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;

e) Chủ trì, phối hợp Ban Cơ yếu Chính phủ trong triển khai các biện pháp bảo bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia có sử dụng giải pháp, sản phẩm mật mã của ngành Cơ yếu Việt Nam để bảo vệ bí mật nhà nước.

3. Bộ Quốc phòng chủ trì thẩm định, đánh giá, kiểm tra an ninh mạng đột xuất và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin quân sự 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 bí mật nhà nước trong hệ thống thông tin quan trọng về an ninh quốc gia; 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 do Ban Cơ yếu Chính phủ quản lý.

Điều 16. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trong trường hợp sau đây:

a) Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội;

b) Khi có đề nghị của chủ quản hệ thống thông tin.

2. Đối tượng kiểm tra an ninh mạng bao gồm:

a) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin;

b) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin;

c) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật.

3. Chủ quản hệ thống thông tin có trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức trong các trường hợp quy định tại khoản 1 Điều này.

5. Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ.

Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin.

6. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật.

7. Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng quy định tại Điều này.

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

Điều 17. Phòng ngừa, xử lý thông tin trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội

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 xâm phạm an ninh lãnh thổ, lợi ích của Nhà nước, phá hoại chính sách kinh tế - xã hội, cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Phản ánh sai lệch, không chính xác về đường biên giới quốc gia chủ quyền lãnh thổ quốc gia Việt Nam; đăng tải, truyền đưa hình ảnh sai lệch, không chính xác, không đầy đủ về bản đồ Việt Nam hoặc thể hiện sai chủ quyền quốc gia Việt Nam;

b) Tuyên truyền gây tổn hại trực tiếp hoặc gián tiếp đến quyền, lợi ích hợp pháp của Nhà nước về chính trị, kinh tế, xã hội, uy tín quốc tế;

c) Kêu gọi, kích động phá hoại việc thực hiện các chính sách kinh tế - xã hội, gây cản trở việc thực thi của các chính sách;

d) Kêu gọi, kích động phá hoại cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

4. Thông tin trên không gian mạng có nội dung phá hoại chính sách đoàn kết bao gồm:

a) Gây mâu thuẫn, chia rẽ giữa các tầng lớp nhân dân, giữa nhân dân với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội;

b) Kích động, gây hận thù, kỳ thị, chia rẽ, ly khai dân tộc, xâm phạm quyền bình đẳng trong cộng động các dân tộc Việt Nam;

c) Kích động, gây mâu thuẫn, chia rẽ người theo tôn giáo với người không theo tôn giáo, giữa người theo các tôn giáo khác nhau, chia rẽ các tín đồ tôn giáo với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội;

d) Phá hoại, cản trở việc thực hiện chính sách đoàn kết quốc tế.

5. Thông tin trên không gian mạng có nội dung xâm phạm quyền, lợi ích hợp pháp của cá nhân bao gồm:

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

b) Xuyên tạc sai sự thật, gây ảnh hưởng đến danh dự, uy tín, nhân phẩm của người khác;

c) Bịa đặt hoặc lan truyền những điều biết rõ là sai sự thật gây thiệt hại đến quyền, lợi ích hợp pháp của người khác;

d) Bịa đặt người khác phạm tội và tố cáo họ trước cơ quan có thẩm quyền;

đ) Mạo danh, giả mạo thông tin, hình ảnh, giọng nói của cá nhân, gây ảnh hưởng đến uy tín, danh dự, nhân phẩm của cá nhân.

6. Thông tin trên không gian mạng có nội dung xâm phạm quyền, lợi ích hợp pháp của tổ chức bao gồm:

a) Loan truyền thông tin xuyên tạc, bịa đặt, sai sự thật, gây ảnh hưởng đến uy tín, hoạt động bình thường của tổ chức;

b) Kêu gọi, vận động, xúi giục tẩy chay sản phẩm, dịch vụ, hàng hóa, nhãn hàng, thương hiệu của tổ chức, doanh nghiệp, gây thiệt hại về vật chất, uy tín của doanh nghiệp, tổ chức;

c) Mạo danh, giả mạo thông tin, hình ảnh, làm nhái sản phẩm, nhãn hiệu hàng hóa, thương hiệu của tổ chức, doanh nghiệp bằng cách sử dụng các tiện ích công nghệ, gây ảnh hưởng đến uy tín của tổ chức, doanh nghiệp.

7. Chủ quản hệ thống thông tin, 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 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 khoản 1, 2, 3, 4, 5 và 6 Điều này trên hệ thống thông tin thuộc phạm vi quản lý hoặc khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng.

8. 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, 5 và 6 Điều này.

9. 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 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, 5 và 6 Điều này.

10. 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, 5 và 6 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.

Điều 18. 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 về an ninh 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 về an ninh quốc gia;

c) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh 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 về an ninh 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 46 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.

Điều 19. Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội

1. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, bao gồm:

a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3 và 4 Điều 22;

b) Thực hiện hành vi quy định tại khoản 1 Điều 23 của Luật này.

2. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để xâm phạm trật tự, an an toàn xã hội bao gồm:

a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 5 và 6 Điều 22 của Luật này;

b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái

phép các phương tiện thanh toán; làm giả con dấu, tài liệu hoặc giấy tờ khác của cơ quan, tổ chức;

d) Tuyên truyền, quảng cáo, 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; động vật hoang dã, nguy cấp, quý, hiếm và các hàng hóa, dịch vụ khác thuộc danh mục cấm theo quy định của pháp luật; môi giới mại dâm; truyền bá văn hóa phẩm đồi trụy; lạm dụng tình dục trẻ em; quấy rối tình dục;

đ) Thiết lập, cung cấp dịch vụ hoặc hỗ trợ vận hành, kinh doanh, giao dịch, mua bán, tiếp thị trực tuyến cho sàn giao dịch, website, ứng dụng trái phép trên không gian mạng, bao 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;

e) Sử dụng danh tính giả, thông tin của người khác, giấy tờ, 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; 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;

g) Quảng cáo, buôn bán hàng giả, 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;

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

l) Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao vi phạm pháp luật về trật tự, an toàn xã hội.

3. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, Bộ Quốc phòng và cơ quan chức năng liên quan có trách nhiệm thực hiện các biện pháp quy định tại khoản 1 Điều 6 của Luật này để đấu tranh, phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để vi phạm pháp luật về trật tự, an toàn xã hội.

4. Chính phủ quy định chi tiết về phòng, chống tội phạm sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao xâm phạm trật tự, an toàn xã hội.

Điều 20. 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, tương tác 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 hoặc xâm phạm đến trẻ em hoặc xâm phạm quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em hoặc xâm phạm đến trẻ em hoặc xâm phạm đến 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, con cái, 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.

Điều 21. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại

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

2. Chủ quản hệ thống thông tin quan trọng về an ninh 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. Tổ chức, 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.

Điều 22. 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, địa phương 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 thuộc Ban Cơ yếu Chính phủ.

Điều 23. 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.

Điều 24. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

1. Tình huống nguy hiểm về an ninh mạng 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 vào hệ thống thông tin quan trọng về an ninh quốc gia;

c) Tấn công 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 về an ninh 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. Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm:

a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng;

d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế;

e) Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng;

g) Biện pháp khác theo quy định của Luật An ninh quốc gia.

4. Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau:

a) Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và áp dụng ngay các biện pháp quy định tại điểm a và điểm b khoản 3 Điều này;

b) Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể.

Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

c) Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp quy định tại khoản 3 Điều này để xử lý tình huống nguy hiểm về an ninh mạng;

d) Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

Điều 25. 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) Giám sát thông tin mạng và phòng ngừa, đấu tranh, xử lý tổ chức, cá nhân có hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh 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.

Điều 26. 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 IV
HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Điều 27. Phân loại thông tin

1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo mức độ nhạy cảm của thông tin, theo tính chất và lĩnh vực của thông tin, theo tình trạng và sự thay đổi của thông tin, theo mức độ quyền truy cập 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.

Điều 28. 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. Nhà cung cấp dịch vụ 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;

đ) Áp dụng cơ chế kiểm soát tự động để kiểm soát việc gửi thông tin trên mạng;

e) Tăng cường bảo mật thông tin liên quan đến giao dịch trực tuyến để bảo đảm an toàn cho các giao dịch thông qua các phương thức xác thực đa yếu tố, mã hóa thông tin và bảo vệ thông tin tài chính của người dùng khi gửi, nhận thông tin giao dịch trực tuyến;

g) Cung cấp thông tin đầy đủ về quyền và nghĩa vụ của người tiếp nhận thông tin khi họ từ chối thông tin, cũng như các hậu quả và quyền lợi liên quan đến việc tiếp nhận hoặc từ chối nhận thông tin.

Điều 29. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;

b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý;

c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng;

d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ;

đ) Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin;

e) Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

2. Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

Điều 30. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế

1. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

2. Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế có trách nhiệm sau đây:

a) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền;

b) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.

Điều 31. Bảo đảm an ninh thông tin 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 được quy định tại khoản 1, 2, 3, 4 Điều 22 và khoản 1 Điều 23 Luật này và thông tin khác có nội dung xâm phạm an ninh quốc gia.

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 chậm nhất là 24 giờ 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; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, đe dọa tính mạng con người, yêu cầu cung cấp thông tin chậm nhất là 03 giờ;

b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm quy định của Luật này 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 pháp luật; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, yêu cầu ngăn chặn, xóa bỏ thông tin chậm nhất là 06 giờ;

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 đối với thông tin có nội dung quy định tại khoản 1, 2, 3, 4 Điều 20 và khoản 1, 2 Điều 21 Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an;

d) Lưu trữ thông tin cá nhân của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tạo ra, bao gồm: tên tài khoản, thời gian sử dụng dịch vụ, thông tin thanh toán phí sử dụng dịch vụ, địa chỉ IP truy cập và các dữ liệu liên quan

khác trong thời gian theo quy định của pháp luật sau khi người dùng kết thúc việc sử dụng dịch vụ.

3. Doanh nghiệp trong nước và ngoài nước 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 về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải áp dụng các biện pháp bảo vệ dữ liệu theo quy định của pháp luật và lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.

Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

4. Chính phủ quy định chi tiết khoản 2 và khoản 3 Điều này.

Điều 32. Bảo đảm an ninh dữ liệu

1. Đối với dữ liệu cốt lõi, dữ liệu quan trọng, cơ quan, tổ chức thiết lập cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ dữ liệu có trách nhiệm:

a) Thiết lập quy trình, quy định nội bộ về bảo vệ an ninh dữ liệu;

b) Áp dụng biện pháp, tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật về bảo vệ an ninh mạng, bảo vệ dữ liệu cá nhân, mật mã, mã hóa, phân quyền truy cập, kiểm tra giám sát truy cập, sao lưu và khôi phục dữ liệu;

c) Có cơ chế kiểm soát chặt chẽ nhân sự trực tiếp tham gia xử lý dữ liệu;

d) Kiểm tra, đánh giá rủi ro định kỳ nhằm phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ đe dọa an ninh dữ liệu;

đ) Không chuyển dữ liệu cốt lõi, dữ liệu quan trọng cho bên thứ ba theo quy định của Luật Dữ liệu và Luật Bảo vệ dữ liệu cá nhân.

2. Trách nhiệm kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra, đánh giá việc chuyển dữ liệu xuyên biên giới; điều kiện đảm bảo an ninh dữ liệu trong hệ thống thông tin quan trọng về an ninh quốc gia, các cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ dữ liệu của cơ quan, tổ chức trừ trường hợp quy định tại điểm b khoản này;

b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu trong hệ thống thông tin quân sự, các cơ sở dữ liệu, trung tâm dữ liệu, hệ thống lưu trữ dữ liệu thuộc Bộ Quốc phòng quản lý.

3. Chính phủ quy định chi tiết Điều này.

Chương V
TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN NINH MẠNG

Điều 33. 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 về an ninh mạng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh 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 về an ninh mạng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng được xây dựng, ban hành và áp dụng tại Việt Nam.

Điều 34. 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 hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh 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 hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh 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 hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh 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 hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh 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; thẩm định quy chuẩn kỹ thuật 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 về an ninh mạng;

b) Xây dựng và ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng;

c) Quản lý chất lượng sản phẩm, dịch vụ an ninh mạng;

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.

Điều 35. 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 về an ninh 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 do Bộ trưởng Bộ Công an chỉ định.

3. 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 VI
KINH DOANH SẢN PHẨM, DỊCH VỤ AN NINH MẠNG

Điều 36. 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 tư vấn an ninh mạng;

đ) Dịch vụ giám sát an ninh mạng;

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

g) Dịch vụ khôi phục dữ liệu;

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

i) 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 mật mã dân sự và các danh mục sản phẩm, dịch vụ an ninh mạng khác quy định tại khoản 1 và khoản 2 Điều này.

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

Điều 37. 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 và d khoản 1 và điểm a khoản 2 Điều 41 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 nhân sự chịu trách nhiệm về bảo đảm an ninh mạng đáp ứng yêu cầu về kiến thức, kỹ năng về bảo đảm an ninh mạng, được cơ quan có thẩm quyền chứng nhận theo quy định;

d) Có phương án kinh doanh phù hợp;

đ) Có đăng ký ngành, nghề kinh doanh phù hợp;

e) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng được yêu cầu chuyên môn về an ninh mạng, nhân thân, lý lịch rõ ràng.

2. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ kiểm tra, đánh giá, giám sát 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 cấp, sửa đổi, bổ sung, cấp lại, gia hạn, tạm đình chỉ và thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng.

Điều 38. 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. Định kỳ hằng năm báo cáo Bộ Công an hoặc Ủy ban nhân dân tỉnh, thành phố về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng trước ngày 31 tháng 12.

4. 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.

5. 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.

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

Điều 39. 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.

4. Chính phủ quy định chi tiết Điều này.

Chương VII
ĐIỀU KIỆN BẢO ĐẢM AN NINH MẠNG

Điều 40. 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.

Điều 41. 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) Chỉ đạo xây dựng tiêu chuẩn, quy chuẩn kỹ thuật đối với các sản phẩm phần cứng, phần mềm nhằm chủ động loại bỏ các nguy cơ về an ninh mạng ngay từ khi hình thành sản phẩm;

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

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

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

đ) 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.

Điều 42. 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 về an ninh quốc gia.

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

Điều 43. 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.

Điều 44. 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.

Điều 45. 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 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 tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý.

Điều 46. 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.

Điều 47. Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng

1. Lực lượng bảo vệ an ninh mạng quy định tại khoản 1 và khoản 2 Điều 47 Luật này phải đáp ứng yêu cầu kiến thức, kỹ năng về bảo đảm an ninh mạng.

2. Người trực tiếp quản trị, vận hành hệ thống thông tin cấp độ 3, 4 và 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước phải tham gia sát hạch và được cấp chứng chỉ kiến thức, kỹ năng về bảo đảm an ninh mạng.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan tổ chức triển khai đánh giá, xác nhận đạt yêu cầu và cấp chứng chỉ kiến thức, kỹ năng về bảo đảm an ninh mạng thông qua chương trình bồi dưỡng, sát hạch và cấp chứng chỉ theo từng đối tượng liên quan.

4. Chính phủ quy định chi tiết chuẩn kiến thức, nội dung chương trình bồi dưỡng, thẩm quyền sát hạch, cấp chứng chỉ và lộ trình áp dụng đối với từng đối tượng liên quan.

Điều 48. Kinh phí bảo vệ an ninh mạng

1. Kinh phí bảo vệ an ninh mạng của cơ quan nhà nước, tổ chức chính trị, Mặt trận Tổ quốc Việt Nam và các đơn vị sự nghiệp công lập 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, về đầu tư công và pháp luật có liên quan.

2. Kinh phí bảo vệ an ninh mạng của cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị phải bảo đảm tối thiểu 10% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin.

3. 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.

Điều 49. Quản lý nhà nước về an ninh mạng

1. Nội dung quản lý nhà nước về an ninh mạng bao gồm:

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

b) Ban hành và tổ chức thực hiện văn bản quy phạm pháp luật về an ninh mạng; xây dựng, ban hành tiêu chuẩn quy chuẩn kỹ thuật an ninh mạng;

c) Quản lý hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng;

d) Quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy về an ninh mạng;

đ) Quản lý tiêu chuẩn về an ninh mạng với hoạt động đầu tư, mua sắm sản phẩm công nghệ phục vụ dự án công, dự án trọng điểm.

e) Quản lý công tác giám sát an ninh mạng;

g) Thẩm định về an ninh mạng trong hồ sơ thiết kế hệ thống thông tin;

h) Tuyên truyền, phổ biến pháp luật về an ninh mạng;

i) 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;

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

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

m) Kiểm tra định kỳ, kiểm tra đột xuất với cơ quan, tổ chức, cá nhân Việt Nam và nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng tại Việt Nam.

n) Hợp tác quốc tế về an ninh mạng.

2. Trách nhiệm quản lý nhà nước về an ninh mạng

a) Chính phủ thống nhất quản lý nhà nước về an ninh mạng;

b) Bộ Công an là cơ quan đầu mối giúp Chính phủ thực hiện quản lý nhà nước về an ninh mạng, trừ quy định tại điểm c khoản này;

c) 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.

d) 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;

e) 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.

Chương VIII
TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN TRONG BẢO ĐẢM AN NINH MẠNG

Điều 50. Trách nhiệm của Bộ Công an

1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng.

2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng.

3. Phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam quy định tại khoản 1 Điều 36 của Luật này.

4. Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về an ninh mạng trên dịch vụ, hệ thống thông tin do doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý.

5. Phòng ngừa, đấu tranh với hoạt động sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm mạng.

6. Bảo đảm an ninh thông tin trên không gian mạng, an ninh dữ liệu; xây dựng cơ chế quản lý định danh IP; xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin an ninh mạng, nguy cơ đe dọa an ninh mạng.

7. Tham mưu, đề xuất Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều Bộ, ngành.

8. Trưng dụng chuyên gia, nhà khoa học, cán bộ chuyên sâu và hệ thống trong trường hợp khẩn cấp để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội trên không gian mạng.

9. Tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

10. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng, an ninh thông tin, an ninh dữ liệu.

Điều 51. Trách nhiệm của Bộ Quốc phòng

1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý.

2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong phạm vi quản lý.

3. Phòng ngừa, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia trong phạm vi quản lý.

4. Phối hợp với Bộ Công an tổ chức diễn tập phòng, chống tấn công mạng, diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, triển khai thực hiện công tác bảo vệ an ninh mạng.

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

Điều 52. Trách nhiệm của Ban Cơ yếu Chính phủ

1. Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ an ninh mạng thuộc phạm vi Ban Cơ yếu Chính phủ quản lý.

2. Bảo vệ an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp theo quy định của Luật này.

3. Thống nhất quản lý nghiên cứu khoa học, công nghệ mật mã; sản xuất, sử dụng, cung cấp sản phẩm mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

Điều 53. Trách nhiệm của Bộ, ngành, Ủy ban nhân dân các cấp

Trong phạm vi nhiệm vụ, quyền hạn của mình, Bộ, ngành, Ủy ban nhân dân các cấp có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin thuộc phạm vi quản lý; phối hợp với lực lượng Công an nhân dân cấp tương ứng thực hiện quản lý nhà nước về an ninh mạng của Bộ, ngành, địa phương.

Điều 54. Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng

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. Kết nối hệ thống giám sát an ninh mạng, hệ thống phòng chống mã độc tập trung về Trung tâm An ninh mạng quốc gia của Bộ Công an hoặc Trung tâm An ninh mạng của tỉnh để hỗ trợ giám sát an ninh mạng.

3. Báo cáo sự cố an ninh mạng với cơ quan chuyên trách của Bộ Công an hoặc Bộ Quốc phòng.

4. 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.

Điều 55. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng

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

2. 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.

3. 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.

4. 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.

5. Có trách nhiệm định danh địa chỉ internet (địa chỉ IP) của tổ chức, cá nhân sử dụng dịch vụ internet, cung cấp cho lực lượng chuyên trách bảo vệ an ninh mạng để quản lý phục vụ công tác đảm bảo an ninh mạng.

6. Phối hợp, thực hiện theo yêu cầu, hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để thiết lập hệ thống kết nối, đấu nối đường truyền kỹ thuật, truyền tải dữ liệu và đáp ứng các điều kiện cần thiết khác để triển khai các giải pháp, biện pháp bảo vệ an ninh mạng.

7. 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 Điều này, khoản 2 và khoản 3 Điều 36 của Luật này.

Điều 56. 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. 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.

3. 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.

4. Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng.

Chương IX
ĐIỀU KHOẢN THI HÀNH

Điều 57. Hiệu lực thi hành

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

2. Luật An toàn thông tin mạng số 86/2015/QH13 ban hành ngày 19 tháng 11 năm 2015 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018 hết hiệu lực kể từ ngày Luật này có hiệu lực thi hành, trừ trường hợp quy định tại Điều 58 của Luật này.

Điều 58. Điều khoản chuyển tiếp

1. 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 ứng với quy định cấp độ mới trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

2. 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.

3. Các phương án, quy trình, thủ tục bảo đảm an toàn thông tin được ban hành theo Luật An toàn thông tin mạng số 86/2015/QH13 ban hành ngày 19 tháng 11 năm 2015 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 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.

4. 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.

5. Chính phủ quy định chi tiết Điều này.

Luật này được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XV, Kỳ họp thứ 10 thông qua ngày tháng 12 năm 2025.

CHỦ TỊCH QUỐC HỘI

Trần Thanh Mẫn