QUỐC HỘI

Luật số: 116/2025/QH15

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
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 và đối tượng áp dụng

1. Luật này quy định về an ninh mạng, bảo vệ an ninh mạng; quyền, nghĩa vụ, trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

2. Luật này áp dụng đối với:

a) Cơ quan, tổ chức, cá nhân Việt Nam;

b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam và người gốc Việt Nam chưa xác định được quốc tịch đang sinh sống tại Việt Nam đã được cấp giấy chứng nhận căn cước;

c) 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 2. Giải thích từ ngữ

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

1. *An ninh mạng* là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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.

2. *An ninh thông tin mạng* là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin trên không gian mạng, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

3. *An ninh dữ liệu* là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá

hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

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

5. *Không gian mạng* là môi trường được hình thành bởi hệ thống 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.

6. *Không gian mạng quốc gia* là phần không gian mạng thuộc chủ quyền, quyền tài phán và quyền kiểm soát của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

7. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và 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.

8. *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.

9. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc 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.

10. *Phần cứng độc hại* là các bộ phận vật lý được thiết kế có chủ đích hoặc được gắn thêm ngoài cấu thành của phần cứng tiêu chuẩn nhằm thu thập thông tin, dữ liệu trái phép hoặc can thiệp, gây ngừng trệ, tê liệt, phá hoại hệ thống máy tính, hệ thống thông tin.

11. *Nhật ký hệ thống* là tập hợp các bản ghi phản ánh thời gian, người dùng, hoạt động, trạng thái của hệ thống phục vụ cho quản lý, giám sát và bảo mật hệ thống.

12. *Tội phạm mạng* là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do cá nhân hoặc tổ chức thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử.

13. *Tấn công mạng* là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử để chiếm đoạt thông tin, gây rối loạn, gián đoạn, tê liệt hoạt động, phá hoại hoặc kiểm soát hệ thống 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.

14. *Khủng bố mạng* là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử nhằm gây hoảng sợ trong công chúng hoặc làm mất ổn định chính trị.

15. *Gián điệp mạng* là hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin hoặc phương tiện điện tử bí mật xâm nhập để

chiếm đoạt, thu thập, sao chép thông tin thuộc phạm vi bí mật nhà nước, dữ liệu quan trọng của cơ quan, tổ chức, cá nhân nhằm mục đích gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

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

17. *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.

18. *Tình huống nguy hiểm về an ninh mạng* là trạng thái hoặc diễn biến trên không gian mạng khi có yếu tố tấn công, xâm nhập, kích động, làm lộ, mất thông tin hoặc hành vi khác đe dọa xâm phạm nghiêm trọng đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

19. *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.

20. *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 nhằm bảo đảm an ninh thông tin cho cơ quan, tổ chức, cá nhân.

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

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

23. *Hệ thống thông tin cơ yếu* là hệ thống thông tin dùng mật mã cơ yếu để bảo vệ thông tin thuộc phạm vi bí mật nhà nước để phục vụ hoạt động chuyên môn nghiệp vụ cơ yếu do tổ chức cơ yếu trực tiếp quản lý, vận hành.

Điều 3. Chính sách của Nhà nước về an ninh mạng

1. 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.

2. Ưu tiên bảo vệ an ninh mạng trong các lĩnh vực quốc phòng, an ninh, cơ yếu, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại.

3. Ưu tiên bố trí nguồn lực xây dựng, phát triển lực lượng chuyên trách bảo vệ an ninh mạng, bảo đảm nguồn nhân lực chất lượng cao phục vụ 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 hoạt động nghiên cứu, phát triển khoa học, công nghệ hiện đại phục vụ bảo vệ an ninh mạng; có cơ chế đặc thù, chính sách ưu đãi để huy động, thu hút, đào tạo và sử dụng nhân tài trong lĩnh vực an ninh mạng.

4. Đẩy mạnh liên kết, đầu tư theo phương thức đối tác công tư trong bảo vệ an ninh mạng; khuyến khích, tạo điều kiện để cơ quan, 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; sử dụng sản phẩm, dịch vụ an ninh mạng của Việt Nam.

5. Mở rộng hợp tác quốc tế về an ninh mạng để tăng cường khả năng bảo vệ an ninh mạng; phòng, chống tội phạm mạng và các mối đe dọa về an ninh mạng xuyên quốc gia; tiếp thu công nghệ hiện đại nhằm nâng cao năng lực tự chủ an ninh mạng quốc gia.

Điều 4. 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 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 bảo vệ an ninh mạng với phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, bảo vệ dữ liệu cá nhân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động hợp pháp trên không gian mạng.

4. Áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại mọi hoạt động 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; xử lý kịp thời, nghiêm minh các hành vi vi phạm pháp luật về an ninh mạng.

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.

Điều 5. 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 thông tin mạng, an ninh dữ liệu, 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 an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

2. Chính phủ quy định chi tiết 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 6. 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 hợp tác, phối hợp trong bảo vệ an ninh mạng; đàm phán, 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 mạng, tội phạm sử dụng công nghệ cao; phối hợp điều tra, xử lý vi phạm pháp luật, tội phạm mạng và tội phạm sử dụng công nghệ cao;

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 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. Trách nhiệm hợp tác quốc tế về an ninh mạng được quy định như sau:

a) Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng;

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

c) 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;

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

đ) 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.

Điều 7. Các hành vi bị nghiêm cấm về an ninh mạng

1. Đăng tải, phát tán thông tin có nội dung sau trên không gian mạng:

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, thông tin sai sự thật, xâm phạm nhân phẩm, danh dự, uy tín 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 bình thường 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 theo phương thức đa cấp, chứng khoán.

2. Thực hiện hành vi sau trên không gian mạng:

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; chiếm đoạt, mua bán, thu giữ, cố ý làm lộ 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, các bộ phận cơ thể 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, tài sản mã hóa, tài sản số 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;

g) Sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; tạo lập, đăng tải, phát tán thông tin quy định tại khoản 1 Điều này;

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

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

k) Thực hiện hành vi khác trên không gian mạng bằng việc sử dụng 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 hoặc phát tán thư rác, tin nhắn rác, cuộc gọi rác, chương trình tin học gây hại đến 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.

5. 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.

6. 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.

7. 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.

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

Chương II
BẢO VỆ AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN

Điều 8. Phân loại cấp độ hệ thống thông tin

1. Hệ thống thông tin được phân loại theo 5 cấp độ căn cứ vào mức độ tổn hại tới an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, cá nhân, lợi ích công cộng khi bị sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng như sau:

a) Cấp độ 1 có thể làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

b) Cấp độ 2 có thể 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;

c) Cấp độ 3 có thể làm tổn hại đặc biệt nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân; tổn hại nghiêm trọng tới lợi ích công cộng; tổn hại hoặc tổn hại nghiêm trọng tới trật tự, an toàn xã hội hoặc làm tổn hại tới an ninh quốc gia;

d) Cấp độ 4 có thể 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 an ninh quốc gia;

đ) Cấp độ 5 có thể làm tổn hại đặc biệt nghiêm trọng tới an ninh quốc gia.

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

Điều 9. 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 có vai trò chiến lược, đặc biệt quan trọng đối với chính trị, quốc phòng, an ninh, ngoại giao, kinh tế, xã hội khi bị sự cố hoặc có hành vi vi phạm pháp luật về an ninh mạng có thể gây tổn hại tới an ninh quốc gia, tổn hại nghiêm trọng đến trật tự, an toàn xã hội, thuộc danh mục do Thủ tướng Chính phủ quyết định.

2. Hệ thống thông tin quan trọng về an ninh quốc gia thuộc các lĩnh vực sau đây:

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;

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, nông nghiệp, tài nguyên và môi trường, hóa chất, y tế, văn hóa;

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 an ninh mạng, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra an ninh mạng, giám sát an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

4. Bộ Công an chủ trì, phối hợp với các Bộ, ngành, cơ quan, tổ chức, cá nhân có liên quan lập, trình Thủ tướng Chính phủ xem xét, quyết định danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

5. Chính phủ quy định chi tiết tiêu chí xác định hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 10. Nhiệm vụ, biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin

1. Nhiệm vụ bảo vệ an ninh mạng đối với 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. Biện pháp bảo vệ an ninh mạng 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 về 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.

3. Chủ quản hệ thống thông tin thuộc Cấp độ 1, Cấp độ 2 thực hiện đầy đủ các nhiệm vụ quy định tại khoản 1 Điều này và theo nhu cầu, khả năng thực tế lựa chọn áp dụng biện pháp quy định tại khoản 2 Điều này.

4. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4 không thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia thực hiện đầy đủ các nhiệm vụ quy định tại khoản 1 Điều này, các biện pháp quy định tại các điểm a, d, đ, e, g và h khoản 2 Điều này và theo nhu cầu, khả năng thực tế lựa chọn áp dụng biện pháp quy định tại điểm b và điểm c khoản 2 Điều này.

5. Chủ quản hệ thống thông tin thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia thực hiện đầy đủ các nhiệm vụ, biện pháp quy định tại khoản 1 và khoản 2 Điều này.

6. Chính phủ quy định chi tiết khoản 1 và khoản 2 Điều này.

Điều 11. 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 5 Điều 10 của Luật này;

b) Khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia phải thực hiện kiểm tra an ninh mạng trước khi đi vào vận hành, khai thác; định kỳ hằng năm, tự kiểm tra an ninh mạng, đánh giá điều kiện 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 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 thuộc Ban Cơ yếu Chính phủ 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 để 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; 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 vệ hệ thống thông tin quan trọng về an ninh quốc gia có sử dụng giải pháp, sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ bí mật nhà nước.

3. Bộ Quốc phòng chủ trì thẩm định an ninh mạng, đánh giá điều kiện an ninh mạng, 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 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 cơ yếu để bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng, đánh giá điều kiện an ninh mạng, 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 thuộc Ban Cơ yếu Chính phủ.

Điều 12. 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 được quy định tại các khoản 12, 13, 14 và 15 Điều 2 của Luật này;

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

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

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

5. 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 13. Các thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. Thông tin 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 bao gồm:

a) Tuyên truyền thông tin, tài liệu có nội dung xuyên tạc, bôi nhọ, 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;

d) 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;

đ) 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 bình thường của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

e) Phản ánh sai lệch, không chính xác về đường biên giới quốc gia, chủ quyền 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.

2. Thông tin có nội dung phá hoại chính sách đoàn kết, chính sách kinh tế - xã hội nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Gây mâu thuẫn, chia rẽ giữa các tầng lớp nhân dân, giữa nhân dân với chính quyền nhân dân, 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 đồng 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, 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;

đ) 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;

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

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

3. Thông tin có nội dung xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân bao gồm:

a) Lan 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 tổ chức, doanh nghiệp;

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;

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

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

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

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

h) 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.

4. Các hành vi thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia và trật tự, 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 1, 2 và 3 Điều này;

b) Thực hiện hành vi quy định tại khoản 1 Điều 15 của Luật này;

c) 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;

d) 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;

đ) 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;

e) 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, trang thông tin điện tử, ứng dụng trái phép trên không gian mạng, bao gồm: sàn thương mại điện tử, trang thông tin điện tử, 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;

g) Sử dụng danh tính giả, giấy tờ, hồ sơ giả hoặc sử dụng trái phép thông tin của người khác 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 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;

h) 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;

k) Hành vi khác thực hiện trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

Điều 14. Phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng

1. 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 1, 2 và 3 Điều 13 của Luật 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.

2. 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 5 của Luật này để xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 và 3 Điều 13 của Luật này và đấu tranh, phòng, chống hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

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 và chủ quản hệ thống thông tin phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 và 3 Điều 13 của Luật này và phòng, chống hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

4. 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 và 3 Điều 13 của Luật 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.

5. Chính phủ quy định chi tiết Điều này.

Điều 15. 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; chiếm đoạt, mua bán, thu giữ, cố ý làm lộ 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, tổ chức 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 trường hợp 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 và 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 1 Điều 30 của Luật này.

5. Bộ Quốc phòng có trách nhiệm thực hiện nội dung quy định tại 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 khoản 4 Điều này đối với hệ thống thông tin cơ yếu thuộc 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 16. Phòng, chống xâm hại trẻ em trên không gian mạng

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

2. Trẻ em sử dụng dịch vụ giá trị gia tăng trên không gian mạng thì cha, mẹ hoặc người giám hộ theo quy định của pháp luật về dân sự đăng ký tài khoản bằng thông tin của cha, mẹ hoặc người giám hộ và có trách nhiệm giám sát, quản lý nội dung trẻ em truy cập, đăng tải và chia sẻ thông tin trên các nền tảng dịch vụ đó.

3. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ giá trị gia tăng trên không gian mạng có các trách nhiệm sau đây:

a) 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 hại trẻ em hoặc xâm phạm quyền trẻ em;

b) Ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em hoặc xâm hại trẻ em hoặc xâm phạm quyền trẻ em;

c) 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;

d) Phối hợp với 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;

đ) Kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

4. 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; phòng, chống xâm hại trẻ em trên không gian mạng.

5. 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 và quy định của Luật này.

6. 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 hại trẻ em, xâm phạm quyền trẻ em.

Điều 17. 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, phát hiện, ngăn chặn phần mềm độc hại và thực hiện 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 tổn hại tới an ninh quốc gia.

Điều 18. 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 19. 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 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 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 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 cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 20. 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 21. 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) Sử dụng giải pháp kỹ thuật để ngăn chặn thông tin vi phạm pháp luật;

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

d) 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;

đ) 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; Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng đối với hệ thống thông tin quân sự.

Điều 22. Ngăn chặn xung đột thông tin trên không gian mạng

1. 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 không gian mạng làm ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội.

2. Ngăn chặn xung đột thông tin trên không gian 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, gỡ bỏ, phản bác, định hướng dư luận, khắc phục, xử phạt và các biện pháp khác loại trừ xung đột thông tin trên không gian mạng.

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

a) Ngăn chặn xung đột thông tin trên không gian mạng 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 hoạt động của tổ chức, cá nhân trong nước và nước ngoài có mục đích tạo xung đột thông tin trên không gian mạng;

c) Loại trừ việc tổ chức thực hiện đăng tải, phát tán thông tin trên không gian 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 Điều này.

Chương IV
HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Điều 23. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội 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 24. 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 25. 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 quy định tại các khoản 1, 2, 3 Điều 13 và khoản 1 Điều 15 của 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 kể từ thời điểm có yêu cầu bằng văn bản hoặc thư điện tử, điện thoại hoặc hình thức trao đổi khác đã được xác nhận để phục vụ xác minh, 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 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 xác minh, 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 các khoản 1, 2 và 3 Điều 13, khoản 1 và khoản 2 Điều 14 của 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 26. Bảo đảm an ninh dữ liệu

1. Bảo đảm an ninh dữ liệu là tổng thể các biện pháp kỹ thuật, tổ chức và pháp lý nhằm bảo vệ dữ liệu, phòng, chống xâm phạm an ninh dữ liệu.

2. Nội dung bảo đảm an ninh dữ liệu bao gồm:

a) Xây dựng chính sách, thiết lập quy trình về bảo đảm an ninh dữ liệu;

b) Áp dụng biện pháp, tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật về an ninh mạng;

c) Sử dụng mật mã cơ yếu, mật mã dân sự để bảo đảm an ninh dữ liệu;

d) Triển khai cơ chế kiểm soát chặt chẽ nhân sự trực tiếp tham gia xử lý dữ liệu;

đ) 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;

e) Kiểm tra, đánh giá việc chuyển dữ liệu xuyên biên giới; điều kiện bảo đảm 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;

g) Các nội dung khác theo quy định của pháp luật.

3. Chính phủ quy định chi tiết khoản 2 Điều này; quy định trách nhiệm bảo đảm an ninh dữ liệu.

Chương V
TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT, SẢN PHẨM, DỊCH VỤ AN NINH MẠNG

Điều 27. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng

1. Tiêu chuẩn an ninh mạng, quy chuẩn kỹ thuật an ninh mạng được áp dụng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ an ninh mạng, công nghệ thông tin và thiết bị kết nối mạng.

2. Việc chứng nhận hợp quy về an ninh mạng, công bố hợp quy về an ninh mạng, chứng nhận hợp chuẩn về an ninh mạng, công bố hợp chuẩn về an ninh mạng thực hiện theo quy định của pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật.

3. 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.

4. Bộ Công an có trách nhiệm sau đây:

a) Xây dựng dự thảo tiêu chuẩn quốc gia về an ninh mạng;

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

c) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng, trừ trường hợp quy định tại khoản 6 Điều này.

5. Bộ trưởng Bộ Công an ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng.

6. Bộ Quốc phòng đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng trong lĩnh vực quân sự.

Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự; đăng ký, chỉ định và quản lý hoạt

động của tổ chức chứng nhận sự phù hợp về an ninh mạng đối với sản phẩm, dịch vụ mật mã dân sự.

Điều 28. Sản phẩm, dịch vụ an ninh mạng

1. Sản phẩm an ninh mạng bao 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.

2. Dịch vụ an ninh mạng bao 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.

3. Chính phủ quy định chi tiết Điều này.

Điều 29. Kinh doanh sản phẩm, dịch vụ an ninh mạng

1. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng phải có giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng.

2. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng có trách nhiệm sau đây:

a) Thực hiện đúng giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; tuân thủ quy định của pháp luật về an ninh mạng và quy định khác của pháp luật có liên quan;

b) Bảo đảm về chất lượng sản phẩm, dịch vụ an ninh mạng đúng với tiêu chuẩn công bố áp dụng, quy chuẩn kỹ thuật tương ứng theo quy định của pháp luật về chất lượng sản phẩm, hàng hóa, pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật trước khi lưu thông trên thị trường;

c) Lập, lưu giữ và bảo mật thông tin của khách hàng, quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, hoạt động cung cấp dịch vụ theo quy định của pháp luật;

d) 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;

đ) Phối hợp, tạo điều kiện, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện các biện pháp bảo vệ an ninh mạng.

3. Chính phủ quy định việc cấp, tạm đình chỉ, thu hồi giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; quy định việc nhập khẩu, xuất khẩu sản phẩm an ninh mạng; quy định việc kinh doanh sản phẩm, dịch vụ an ninh mạng.

Chương VI
LỰC LƯỢNG, ĐIỀU KIỆN BẢO ĐẢM AN NINH MẠNG

Điều 30. Lực lượng bảo vệ an ninh mạng

1. Lực lượng bảo vệ an ninh mạng bao gồm:

a) Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng;

b) 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;

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

2. Chính phủ quy định chi tiết khoản 1 Điều này; quy định việc phối hợp giữa các lực lượng bảo vệ an ninh mạng.

Điều 31. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng

1. Nhà nước đào tạo, phát triển nguồn nhân lực bảo vệ an ninh mạng bảo đảm số lượng, chất lượng, đáp ứng yêu cầu năng lực bảo vệ an ninh mạng quốc gia.

2. Lực lượng chuyên trách bảo vệ an ninh mạng được ưu tiên bố trí nhân lực theo vị trí việc làm, tiêu chuẩn chức danh, được áp dụng cơ chế tuyển dụng, xét tuyển, sử dụng, đào tạo, bồi dưỡng, đãi ngộ và thu hút nhân tài theo chính sách đặc thù do Chính phủ quy định.

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

a) Bố trí bộ phận hoặc nhân sự chuyên trách phù hợp với cấp độ bảo vệ của hệ thống;

b) Bảo đảm người thực hiện nhiệm vụ an ninh mạng đáp ứng tiêu chuẩn chuyên môn, nghiệp vụ;

c) Thường xuyên bồi dưỡng, cập nhật kỹ năng cho đội ngũ nhân sự liên quan đến vận hành, giám sát, ứng cứu và xử lý sự cố mạng.

Điều 32. 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; phát hiện tài năng trẻ về an ninh mạng, công nghệ thông tin để định hướng học tập, tuyển chọn, thu hút và sử dụng trong lĩnh vực an ninh mạng.

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

Điều 34. Tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng

1. Lực lượng bảo vệ an ninh mạng quy định tại điểm a và điểm b khoản 1 Điều 30 của Luật này phải đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng.

2. Người trực tiếp quản trị, vận hành hệ thống thông tin Cấp độ 3, Cấp độ 4, Cấp độ 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước phải được tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng và được cấp chứng nhận, trừ các cá nhân đã được đào tạo chuyên ngành an ninh mạng.

3. Bộ Công an chủ trì, phối hợp với các Bộ, ngành liên quan tổ chức tập huấn về kiến thức, kỹ năng chuyên sâu về an ninh mạng, trừ trường hợp quy định tại khoản 4 Điều này.

4. Bộ Quốc phòng, Ban Cơ yếu Chính phủ tổ chức tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng đối với đối tượng thuộc phạm vi quản lý.

5. Chính phủ quy định về chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng; chương trình, nội dung, việc chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng.

Điều 35. 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; ưu tiên phổ biến, hướng dẫn trẻ em, người cao tuổi, người khó khăn trong nhận thức để nâng cao khả năng tự bảo vệ quyền và lợi ích hợp pháp của mình trên không gian 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 36. 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 37. 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 chính sách, chiến lược, quy hoạch phát triển công nghiệp an ninh mạng; 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 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, tối ưu hóa sử dụng nguồn nhân lực an ninh mạng chất lượng cao;

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.

3. Hoạt động đầu tư, thu hút nguồn lực phát triển hạ tầng công nghiệp an ninh mạng bao gồm:

a) Hoạt động đầu tư xây dựng hạ tầng công nghiệp an ninh mạng là ngành, nghề đặc biệt ưu đãi đầu tư, được hưởng ưu đãi, hỗ trợ theo quy định của pháp luật về đầu tư, thuế, đất đai và pháp luật khác có liên quan;

b) Nhà nước ưu tiên bố trí nguồn vốn ngân sách để đầu tư xây dựng hạ tầng công nghiệp an ninh mạng gồm: Cơ sở nghiên cứu, thiết kế, sản xuất, thử nghiệm sản phẩm, dịch vụ an ninh mạng; Phòng thí nghiệm trọng điểm quốc gia về an ninh mạng; Cơ sở đo kiểm, thử nghiệm, đánh giá sản phẩm, dịch vụ an ninh mạng; Trung tâm dữ liệu lớn; Khu công nghiệp an ninh mạng tập trung; Tổ hợp công nghiệp an ninh mạng;

c) Hạ tầng công nghiệp an ninh mạng được nhà nước đầu tư quy định tại điểm b khoản này là một loại tài sản kết cấu hạ tầng và được quản lý, khai thác, vận hành theo quy định của pháp luật về quản lý, sử dụng tài sản công;

d) Tổ chức, doanh nghiệp được nhập khẩu dây chuyền công nghệ, thiết bị, máy móc, công cụ phục vụ hoạt động đào tạo, nghiên cứu và phát triển sản phẩm, dịch vụ an ninh mạng;

đ) Các cơ quan, tổ chức, doanh nghiệp nhà nước ưu tiên sử dụng các sản phẩm, dịch vụ an ninh mạng được sản xuất trong nước.

4. Bộ Công an tham mưu, giúp Chính phủ xây dựng, phát triển hạ tầng công nghiệp an ninh mạng nhằm nâng cao năng lực tự chủ về an ninh mạng.

Điều 38. Kinh phí bảo vệ an ninh mạng

1. Cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội và các đơn vị sự nghiệp công lập do ngân sách nhà nước bảo đảm phải bố trí kinh phí bảo vệ an ninh mạng trong dự toán chi thực hiện nhiệm vụ chuyển đổi số, ứng dụng công nghệ thông tin hàng năm của cơ quan, tổ chức, đơn vị mình; bố trí tối thiểu 15% tổng kinh phí thực hiện chương trình, đề án, dự án đầu tư chuyển đổi số, ứng dụng công nghệ thông tin để bảo vệ an ninh mạng.

2. Cơ quan, tổ chức, đơn vị không thuộc quy định tại khoản 1 Điều này tự bảo đảm kinh phí bảo vệ an ninh mạng cho cơ quan, tổ chức, đơn vị mình.

Chương VII
TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN VỀ AN NINH MẠNG

Điều 39. 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 là cơ quan đầu mối giúp Chính phủ thực hiện quản lý nhà nước về an ninh mạng; chịu trách nhiệm trước Chính phủ thực hiện các nội dung quản lý nhà nước về an ninh mạng sau đây, trừ nội dung quy định tại khoản 3 và khoản 4 Điều này:

a) Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành văn bản quy phạm pháp luật về an ninh mạng;

b) Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; nghiên cứu, xây dựng, phát triển, sử dụng mật mã an ninh để bảo vệ an ninh dữ liệu thuộc phạm vi quản lý của Bộ Công an;

c) 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 13 của Luật này;

d) 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;

đ) 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;

e) Bảo đảm an ninh thông tin trên không gian mạng, an ninh dữ liệu; xây dựng cơ chế quản lý định danh địa chỉ 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;

g) 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;

h) Huy động chuyên gia, nhà khoa học, cán bộ chuyên sâu và trưng dụng hệ thống, phương tiện, thiết bị trong trường hợp khẩn cấp để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội trên không gian mạng;

i) 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;

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

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 như sau:

a) Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý;

b) 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;

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

d) 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;

đ) 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.

4. Ban Cơ yếu Chính phủ giúp 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.

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 tại địa phương; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng.

Điều 40. 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 sau đây:

a) Thực hiện bảo vệ hệ thống thông tin theo quy định tại Luật này;

b) 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, thành phố để hỗ trợ giám sát an ninh mạng;

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

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

a) Có phương án bảo đảm an ninh mạng được cơ quan nhà nước có thẩm quyền thẩm định an ninh mạng 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 41. 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 đối với người sử dụng dịch vụ; xây dựng phương án ứng cứu khẩn cấp bảo đảm an ninh mạng để chủ động xử lý điểm yếu, rủi ro và sự cố an ninh mạng.

3. Khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án ứng cứu khẩn cấp bảo đảm an ninh mạng, đồng thời báo cáo ngay với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này.

4. Áp dụng các biện pháp, giải pháp kỹ thuật để bảo đảm an ninh mạng cho hoạt động xử lý dữ liệu, xử lý dữ liệu cá nhân theo quy định của Luật này, pháp luật về dữ liệu, pháp luật về bảo vệ dữ liệu cá nhân và quy định khác của pháp luật có liên quan.

5. Có trách nhiệm định danh địa chỉ IP của tổ chức, cá nhân sử dụng dịch vụ internet; cung cấp thông tin định danh địa chỉ IP cho lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện biện pháp bảo vệ an ninh mạng.

6. Phối hợp thực hiện theo 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 khi có yêu cầu để phục vụ điều tra, xác minh, xử lý hành vi vi phạm pháp luật về 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 25 của Luật này.

Điều 42. 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 sử dụng tài khoản số để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ của hành vi vi phạm, chủ tài khoản số, người sử dụng tài khoản số 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. 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.

4. 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 43. Sửa đổi, bổ sung một số điều của các luật có liên quan

1. Thay thế một số cụm từ, bãi bỏ một số khoản của Luật Lưu trữ số 33/2024/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" tại điểm b khoản 1 Điều 35, cụm từ "an toàn thông tin mạng" tại điểm b khoản 2 Điều 36 và cụm từ "an toàn, an ninh thông tin" tại khoản 3 Điều 60 bằng cụm từ "an ninh mạng";

b) Bãi bỏ khoản 4 Điều 58.

2. Thay thế, bãi bỏ một số cụm từ của Luật Bảo vệ quyền lợi người tiêu dùng số 19/2023/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" bằng cụm từ "an ninh thông tin" tại điểm d khoản 1 Điều 16; cụm từ "an toàn, an ninh thông tin" bằng cụm từ "an ninh mạng" tại khoản 1 Điều 15, tên Điều 19, khoản 1 và khoản 3 Điều 19;

b) Bãi bỏ cụm từ "an toàn thông tin mạng," tại khoản 3 Điều 19.

3. Thay thế một số cụm từ của Luật Phí và lệ phí số 97/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 09/2017/QH14, Luật số 23/2018/QH14, Luật số 72/2020/QH14, Luật số 16/2023/QH15, Luật số 20/2023/QH15, Luật số 24/2023/QH15, Luật số 33/2024/QH15, Luật số 35/2024/QH15, Luật số 47/2024/QH15, Luật số 60/2024/QH15, Luật số 74/2025/QH15, Luật số 89/2025/QH15, Luật số 94/2025/QH15, Luật số 95/2025/QH15 và Luật số 118/2025/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" bằng cụm từ "an ninh mạng" tại tiểu mục 10 mục VI thuộc phần A và tiểu mục 16 mục III thuộc phần B Phụ lục số 01 - Danh mục phí và lệ phí;

b) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại tiểu mục 11 mục VI thuộc phần A Phụ lục số 01 - Danh mục phí và lệ phí.

4. Thay thế, bãi bỏ một số cụm từ của Luật Công nghiệp công nghệ số số 71/2025/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin" bằng cụm từ "an ninh mạng" tại điểm a khoản 1 Điều 25;

b) Bãi bỏ cụm từ "an toàn thông tin mạng," tại Điều 10.

5. Thay thế, bãi bỏ một số cụm từ của Luật Dữ liệu số 60/2024/QH15 như sau:

a) Thay thế cụm từ "an toàn, an ninh dữ liệu" bằng cụm từ "an ninh dữ liệu" tại khoản 4 Điều 25;

b) Thay thế cụm từ "an ninh, an toàn thông tin" bằng cụm từ "an ninh mạng" tại khoản 2 Điều 33;

c) Bãi bỏ cụm từ ", an toàn thông tin" tại khoản 4 Điều 25;

d) Bãi bỏ cụm từ "an toàn thông tin mạng," tại khoản 4 Điều 39;

đ) Bãi bỏ cụm từ "pháp luật về an toàn thông tin mạng," tại khoản 4 Điều 43.

6. Thay thế, bãi bỏ một số cụm từ của Luật Di sản văn hoá số 45/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 84/2025/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại khoản 4 Điều 59;

b) Bãi bỏ cụm từ "an toàn thông tin mạng," tại điểm c khoản 2 Điều 86.

7. Thay thế, bãi bỏ một số cụm từ của Luật Viễn thông số 24/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 47/2024/QH15 như sau:

a) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh thông tin" tại khoản 8 Điều 5;

b) Bãi bỏ cụm từ ", an toàn thông tin mạng" tại tên Điều 5 và khoản 1 Điều 5, điểm c khoản 2 Điều 38;

c) Bãi bỏ cụm từ "an toàn thông tin mạng," tại khoản 2 Điều 21 và điểm b khoản 2 Điều 29.

8. Thay thế, bãi bỏ một số cụm từ của Luật Giao dịch điện tử số 20/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 60/2024/QH15 như sau:

a) Bãi bỏ cụm từ "an toàn thông tin mạng và" tại tên Điều 5;

b) Bãi bỏ cụm từ "pháp luật về an toàn thông tin mạng," tại khoản 1 Điều 5;

c) Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại điểm c khoản 1 Điều 20, khoản 2 Điều 21, điểm c khoản 1 Điều 29, khoản 6 Điều 30, khoản 4 Điều 44, điểm a khoản 4 Điều 46 và điểm c khoản 1 Điều 47;

d) Bãi bỏ cụm từ "an toàn thông tin mạng," tại điểm d khoản 1 Điều 42 và điểm a khoản 1 Điều 47.

9. Thay thế cụm từ "an toàn thông tin mạng" bằng cụm từ "an ninh mạng" tại điểm b khoản 2 Điều 12 của Luật Thuế thu nhập doanh nghiệp số 67/2025/QH15; tại khoản 1 Điều 169 của Luật Đất đai số 31/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 43/2024/QH15, Luật số 47/2024/QH15, Luật số 58/2024/QH15, Luật số 71/2025/QH15, Luật số 84/2025/QH15, Luật số 93/2025/QH15 và Luật số 95/2025/QH15.

10. Thay thế cụm từ "an ninh, an toàn thông tin" bằng cụm từ "an ninh mạng" tại điểm a khoản 3 Điều 7 của Luật Tài nguyên nước số 28/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 84/2025/QH15.

11. Bãi bỏ cụm từ "an toàn thông tin mạng;" tại điểm đ khoản 1 Điều 24 của Luật Xử lý vi phạm hành chính số 15/2012/QH13 đã được sửa đổi, bổ sung

một số điều theo Luật số 54/2014/QH13, Luật số 18/2017/QH14, Luật số 67/2020/QH14, Luật số 09/2022/QH15, Luật số 11/2022/QH15, Luật số 56/2024/QH15 và Luật số 88/2025/QH15.

12. Bãi bỏ cụm từ "an toàn thông tin mạng," tại khoản 6 Điều 16 của Luật Công an nhân dân số 37/2018/QH14 đã được sửa đổi, bổ sung một số điều theo Luật số 21/2023/QH15, Luật số 30/2023/QH15, Luật số 38/2024/QH15, Luật số 52/2024/QH15 và Luật số 86/2025/QH15; tại khoản 1 Điều 66 của Luật Bầu cử đại biểu Quốc hội và đại biểu Hội đồng nhân dân số 85/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 83/2025/QH15.

13. Bãi bỏ cụm từ ", an toàn thông tin" tại khoản 3 Điều 136 của Luật Tổ chức Tòa án nhân dân số 34/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 81/2025/QH15; tại khoản 1 Điều 26 của Luật Điện lực số 61/2024/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 94/2025/QH15.

14. Bãi bỏ cụm từ "an toàn thông tin," tại khoản 8 Điều 29; cụm từ "an toàn thông tin và" tại khoản 2 và khoản 7 Điều 29 của Luật Hóa chất số 69/2025/QH15.

15. Bãi bỏ cụm từ "an toàn thông tin," tại khoản 3 Điều 51, khoản 1 và khoản 5 Điều 52 của Luật Đấu thầu số 22/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 57/2024/QH15 và Luật số 90/2025/QH15; tại điểm e khoản 1 Điều 23 của Luật Phòng thủ dân sự số 18/2023/QH15 đã được sửa đổi, bổ sung một số điều theo Luật số 98/2025/QH15.

16. Bãi bỏ cụm từ ", pháp luật về bảo đảm an toàn thông tin" tại khoản 4 Điều 7 của Luật Năng lượng nguyên tử số 94/2025/QH15.

17. Bãi bỏ khoản 3 Điều 49 của Luật Thư viện số 46/2019/QH14.

Điều 44. Hiệu lực thi hành

1. Luật này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2026.

2. Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14; Luật An ninh mạng số 24/2018/QH14 hết hiệu lực kể từ ngày Luật này có hiệu lực thi hành.

Điều 45. Điều khoản chuyển tiếp

1. Hệ thống thông tin đã được xác định cấp độ theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 thì tiếp tục giữ cấp độ đã được xác định kể từ ngày Luật này có hiệu lực thi hành; trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành thì phải bảo đảm điều kiện, tiêu chuẩn, biện pháp bảo vệ an ninh mạng tương ứng với cấp độ theo quy định của Luật này.

2. Các loại giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, mật mã dân sự theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14

đã được cấp trước ngày Luật này có hiệu lực thi hành có giá trị sử dụng đến hết thời hạn được ghi trên giấy phép.

3. Các sản phẩm, dịch vụ, giải pháp, phương tiện kỹ thuật bảo đảm an toàn thông tin mạng theo quy định của Luật An toàn thông tin mạng số 86/2015/QH13 đã được sửa đổi, bổ sung một số điều theo Luật số 35/2018/QH14 đã được đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành tiếp tục được sử dụng; trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành thì phải bảo đảm các điều kiện an ninh mạng theo quy định của Luật này.

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

CHỦ TỊCH QUỐC HỘI

Trần Thanh Mẫn