QUỐC HỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Luật số: 24/2018/QH14	

LUẬT
AN NINH MẠNG

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

Quốc hội ban hành Luật An ninh mạng.

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Luật này quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

Điều 2. 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.

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

3. *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.

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

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

a) Hệ thống truyền dẫn bao gồm hệ thống truyền dẫn quốc gia, hệ thống truyền dẫn kết nối quốc tế, hệ thống vệ tinh, hệ thống truyền dẫn của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng;

b) Hệ thống các dịch vụ lõi bao gồm hệ thống phân luồng và điều hướng thông tin quốc gia, hệ thống phân giải tên miền quốc gia (DNS), hệ thống chứng thực quốc gia (PKI/CA) và hệ thống cung cấp dịch vụ kết nối, truy cập Internet của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng;

c) Dịch vụ, ứng dụng công nghệ thông tin bao gồm dịch vụ trực tuyến; ứng dụng công nghệ thông tin có kết nối mạng phục vụ quản lý, điều hành của cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng; cơ sở dữ liệu quốc gia.

Dịch vụ trực tuyến bao gồm chính phủ điện tử, thương mại điện tử, trang thông tin điện tử, diễn đàn trực tuyến, mạng xã hội, blog;

d) Cơ sở hạ tầng công nghệ thông tin của đô thị thông minh, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh và hệ thống trí tuệ nhân tạo.

6. *Cổng kết nối mạng quốc tế* là nơi diễn ra hoạt động chuyển nhận tín hiệu mạng qua lại giữa Việt Nam và các quốc gia, vùng lãnh thổ khác.

7. *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.

8. *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.

9. *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.

10. *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 để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên 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 của cơ quan, tổ chức, cá nhân.

11. *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.

12. *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.

13. *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.

14. *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.

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

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

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

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

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

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

Điều 4. Nguyên tắc bảo vệ an ninh mạng

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

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

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

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

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

6. 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.

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

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) 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;

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

k) 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;

l) 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;

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

n) 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 trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm m và điểm n khoản 1 Điều này.

Điều 6. 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 7. 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 và toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi.

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

a) Nghiên cứu, phân tích xu hướng an ninh mạng;

b) Xây dựng cơ chế, chính sách nhằm đẩy mạnh hợp tác giữa tổ chức, cá nhân Việt Nam với tổ chức, cá nhân nước ngoài, tổ chức quốc tế hoạt động về an ninh mạng;

c) Chia sẻ thông tin, kinh nghiệm; hỗ trợ đào tạo, trang thiết bị, công nghệ bảo vệ an ninh mạng;

d) Phòng, chống tội phạm mạng, hành vi xâm phạm an ninh mạng; ngăn ngừa các nguy cơ đe dọa an ninh mạng;

đ) Tư vấn, đào tạo và phát triển nguồn nhân lực an ninh mạng;

e) Tổ chức hội nghị, hội thảo và diễn đàn quốc tế về an ninh mạng;

g) Ký kết và thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng;

h) Thực hiện chương trình, dự án hợp tác quốc tế về an ninh mạng;

i) 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 8. Các hành vi bị nghiêm cấm về an ninh mạng

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

a) Hành vi quy định tại khoản 1 Điều 18 của Luật này;

b) 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;

c) 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;

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

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

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

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; 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 quan trọng về an ninh quốc gia.

3. 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 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.

4. 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.

5. 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.

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

Điều 9. 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 QUAN TRỌNG VỀ AN NINH QUỐC GIA

Điều 10. 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 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.

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

4. Chính phủ quy định việc phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, các Bộ, ngành chức năng trong việc thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 11. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Thẩm định an ninh mạng là hoạt động xem xét, đánh giá những nội dung về an ninh mạng để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin.

2. Đối tượng thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt;

b) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt.

3. Nội dung thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

a) Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế;

b) Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng.

4. Thẩm quyền thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 12. Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Đánh giá điều kiện về an ninh mạng là hoạt động xem xét sự đáp ứng về an ninh mạng của hệ thống thông tin trước khi đưa vào vận hành, sử dụng.

2. Hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng các điều kiện sau đây về:

a) Quy định, quy trình và phương án bảo đảm an ninh mạng; nhân sự vận hành, quản trị hệ thống;

b) Bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống;

c) Biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng; biện pháp bảo vệ hệ thống điều khiển và giám sát tự động, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh, hệ thống trí tuệ nhân tạo;

d) Biện pháp bảo đảm an ninh vật lý bao gồm cách ly cô lập đặc biệt, chống rò rỉ dữ liệu, chống thu tin, kiểm soát ra vào.

3. Thẩm quyền đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

4. Hệ thống thông tin quan trọng về an ninh quốc gia được đưa vào vận hành, sử dụng sau khi được chứng nhận đủ điều kiện an ninh mạng.

5. Chính phủ quy định chi tiết khoản 2 Điều này.

Điều 13. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin.

2. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện trong trường hợp sau đây:

a) Khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin;

b) Khi có thay đổi hiện trạng hệ thống thông tin;

c) Kiểm tra định kỳ hằng năm;

d) Kiểm tra đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; khi có yêu cầu quản lý nhà nước về an ninh mạng; khi hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

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

b) Quy định, biện pháp bảo vệ an ninh mạng;

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

d) Phương án ứng phó, khắc phục sự cố an ninh mạng của chủ quản hệ thống thông tin;

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

e) Nhân lực bảo vệ an ninh mạng.

4. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý trong trường hợp quy định tại các điểm a, b và c khoản 2 Điều này; thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đối với hệ thống thông tin quân sự.

5. Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau:

a) Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; ít nhất là 72 giờ trong trường hợp có yêu cầu quản lý nhà nước về an ninh mạng hoặc hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng;

b) 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;

c) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, 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 để bảo vệ thông tin thuộc bí mật nhà nước.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ kiểm tra an ninh mạng đột xuất 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 để bảo vệ thông tin thuộc bí mật nhà nước;

d) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất.

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

Điều 14. Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Giám sát an ninh mạng là hoạt động thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý.

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp.

3. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý; 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, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 15. Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm:

a) Phát hiện, xác định sự cố an ninh mạng;

b) Bảo vệ hiện trường, thu thập chứng cứ;

c) Phong tỏa, giới hạn phạm vi xảy ra sự cố an ninh mạng, hạn chế thiệt hại do sự cố an ninh mạng gây ra;

d) Xác định mục tiêu, đối tượng, phạm vi cần ứng cứu;

đ) Xác minh, phân tích, đánh giá, phân loại sự cố an ninh mạng;

e) Triển khai phương án ứng phó, khắc phục sự cố an ninh mạng;

g) Xác minh nguyên nhân và truy tìm nguồn gốc;

h) Điều tra, xử lý theo quy định của pháp luật.

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; 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.

3. Điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an 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, trừ trường hợp quy định tại điểm b và điểm c khoản này; tham gia ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 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;

b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

4. Cơ quan, tổ chức, cá nhân có trách nhiệm tham gia ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu của lực lượng chủ trì điều phối.