

Luật số: /2018/QH14

DỰ THẢO ĐÃ CHỈNH LÝ

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 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, hệ thống máy tính, 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 Nhà nước 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: hệ thống truyền dẫn quốc gia, hệ thống truyền dẫn kết nối quốc tế, hệ thống vệ tinh, hệ thống truyền dẫn của các cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet;

b) Hệ thống các dịch vụ lõi: 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 các hệ thống cung cấp dịch vụ kết nối, truy cập internet của các cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet;

c) Các dịch vụ, ứng dụng công nghệ thông tin: dịch vụ trực tuyến, gồm chính phủ điện tử, thương mại điện tử, trang thông tin điện tử, diễn đàn trực tuyến, mạng xã hội, blog; ứng dụng công nghệ thông tin có kết nối mạng phục vụ quản lý, điều hành của các cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng; cơ sở dữ liệu quốc gia;

d) Các cơ sở hạ tầng công nghệ thông tin của các thành phố thông minh, Internet của 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. *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.

7. *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 hoặc truy cập trái phép máy tính, hệ thống máy tính hoặc hệ thống thông tin.

8. *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.

9. *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, hệ thống máy tính hoặc phương tiện điện tử của cơ quan, tổ chức, cá nhân.

10. *Chiến tranh mạng* là một loại hình chiến tranh do một quốc gia hoặc vùng lãnh thổ tiến hành, diễn ra độc lập trên không gian mạng hoặc kết hợp với hoạt động quân sự xâm phạm độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam.

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

12. *Nguy cơ đe dọa an ninh mạng* là dấu hiệu xuất hiện trên không gian mạng có khả năng trực tiếp xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng, đặc biệt nghiêm trọng tới trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

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

14. *Tình huống nguy hiểm về an ninh mạng* là sự việc xảy ra trên không gian mạng ảnh hưởng nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng tới trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc gây thiệt hại về tính mạng con người.

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

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

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 tổ chức, cá nhân.

3. 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.

4. Xử lý nghiêm minh các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

5. Ưu tiên xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho các lực lượng bảo vệ an ninh mạng và các tổ chức, cá nhân tham gia bảo vệ an ninh mạng.

6. 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 và phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng.

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

8. Ưu tiên đầu tư, bố trí kinh phí để bảo vệ an ninh mạng.

Điều 4. Nguyên tắc bảo vệ an ninh mạng

1. Tuân thủ Hiến pháp, pháp luật, bảo đảm lợi ích Nhà nước, quyền và lợi ích hợp pháp của 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 các 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 tổ chức, cá nhân; sẵn sàng ngăn chặn các mối đe dọa chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

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

6. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

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 ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông công cộng, mạng viễn thông dùng riêng, mạng internet, việc 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;

k) Thu thập dữ liệu điện tử liên quan tới hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của 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, áp dụng các biện pháp ngăn chặn, biện pháp cưỡng chế, biện pháp thu thập chứng cứ theo quy định của Bộ luật Tố tụng hình sự;

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

Điều 6. Xác lập và bảo vệ không gian mạng quốc gia

1. Chính phủ xác lập phạm vi không gian mạng quốc gia.

2. Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của 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 theo nguyên tắc tôn trọng độc lập, chủ quyền quốc gia, 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, các 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 quản lý nhà nước về hợp tác quốc tế về an ninh mạng. Bộ Quốc phòng trong phạm vi nhiệm vụ, quyền hạn của mình 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.

4. Hoạt động hợp tác quốc tế về an ninh mạng của các bộ, ngành khác, của các 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

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

a) Soạn thảo, đăng tải, tán phát thông tin quy định tại các khoản 1, 2, 3, 4 Điều 15; thực hiện hành vi quy định tại khoản 1 Điều 16 và khoản 1 Điều 17 của Luật này;

b) Tổ chức, hoạt động, cấu 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; kỳ thị giới tính, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho các 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 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 cộng đồng;

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

2. Thực hiện chiến tranh mạng, 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 máy tính, mạng viễn thông; phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

4. Chông 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 của 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 tổ chức, cá nhân hoặc để trục lợi.

6. Hành vi khác sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc vi phạm quy định của Luật này.

Chương II

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

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 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 gây phương hại đến an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng tới trật tự, an toàn xã hội.

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 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 kinh tế, năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên môi trường, hóa chất, y tế, văn hóa, báo chí, phát thanh, truyền hình;

h) Hệ thống điều khiển và giám sát tự động tại các 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 Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

4. Chính phủ quy định cơ chế phối hợp giữa các bộ trong thực hiện các nội dung quản lý nhà nước có liên quan đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 10. 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 cần thiết về an ninh mạng để làm cơ sở cho việc quyết định xây dựng hoặc bổ sung, điều chỉnh, nâng cấp hệ thống thông tin.

2. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia tiến hành trong trường hợp sau đây:

a) Đối với báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hoặc đề án nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia trước khi phê duyệt;

b) Đối với dịch vụ an toàn thông tin mạng trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia.

3. Nội dung thẩm định an ninh mạng, bao gồm:

a) Sự phù hợp của phương án bảo vệ an ninh mạng;

b) Sự phù hợp với phương án ứng phó, khắc phục sự cố an ninh mạng;

c) Sự tuân thủ quy định, điều kiện an ninh mạng trong thiết kế;

d) Phương án bố trí nhân lực bảo vệ an ninh mạng.

4. 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 hệ thống thông tin quân sự do Bộ Quốc phòng quản lý và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ. 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. 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 11. 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 đối với hệ thống thông tin trước khi đưa vào vận hành, sử dụng.

2. Điều kiện về an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

- a) Điều kiện về lực lượng nhân sự vận hành, quản trị hệ thống;
- b) Điều kiện về hệ thống các quy định, quy trình và phương án bảo đảm an ninh mạng;
- c) Điều kiện về bảo đảm an ninh đối với các trang thiết bị, phần cứng, phần mềm là thành phần hệ thống;
- d) Điều kiện về triển khai các biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng;
- đ) Điều kiện về triển khai các biện pháp bảo vệ hệ thống điều khiển và giám sát tự động, Internet của 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;
- e) Điều kiện về triển khai các biện pháp bảo đảm an ninh vật lý, gồm: cách ly cô lập đặc biệt, chống rò rỉ dữ liệu, chống thu tin, kiểm soát ra vào;
- g) Các điều kiện đặc thù khác được quy định đối với từng hệ thống thông tin quan trọng về an ninh quốc gia.

3. 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.

4. 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 hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; 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; 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.

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

Điều 12. 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 tải 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 tiến hành trong trường hợp sau đây:

- a) Khi đưa phương tiện điện tử 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; 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, chính sách, biện pháp bảo vệ an ninh mạng;
- c) Thông tin được lưu trữ, xử lý, truyền tải 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) Các biện pháp bảo vệ bí mật nhà nước, 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 tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin do mình quản lý trong các trường hợp quy định tại các điểm a, b và c khoản 2 Điều này, thông báo kết quả bằng văn bản 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 trước tháng 10 hằng năm.

5. Kiểm tra an ninh mạng đột xuất:

a) Trước thời điểm tiến hành kiểm tra an ninh mạng đột xuất, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông tin quan trọng về an ninh quốc gia ít nhất 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng và ít nhất 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) Sau khi tiến hành kiểm tra an ninh mạng đột xuất, 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 quan trọng về an ninh quốc gia trong thời hạn tối đa 30 ngày làm việc kể từ khi kết thúc kiểm tra an ninh mạng đột xuất; hướng dẫn hoặc tham gia khắc phục điểm yếu, lỗ hổng bảo mật khi có đề nghị của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia;

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 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 do Ban Cơ yếu Chính phủ quản lý và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin 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 13. 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 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 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 do mình 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 các 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 14. 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 các phương án xử lý, 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 do mình 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:

- a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an có trách nhiệm 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 hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; 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 các chủ quản hệ thống thông tin quan trọng về an ninh quốc gia 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 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 đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

4. Tổ chức, cá nhân có trách nhiệm 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 của lực lượng chủ trì điều phối.

Chương III

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

Điều 15. Phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế

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

a) Thông tin có nội dung tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Thông tin gây 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) Thông tin xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

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

a) Thông tin có nội dung tuyên truyền, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Thông tin có nội dung tuyên truyền, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở sự hoạt động của cơ quan nhà nước, tổ chức xã hội nhằm chống chính quyền nhân dân hoặc gây mất ổn định về an ninh trật tự.

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

a) Thông tin có nội dung xúc phạm nghiêm trọng nhân phẩm, danh dự của người khác;

b) Thông tin bịa đặt, sai sự thật nhằm xúc phạm nghiêm trọng nhân phẩm, danh dự hoặc gây thiệt hại đến quyền, lợi ích hợp pháp của tổ chức, cá nhân đó.

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

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

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

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

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

7. Cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet và chủ quản hệ thống thông tin có trách nhiệm phối hợp chặt chẽ với cơ quan chức năng xử lý thông tin trên không gian mạng có nội dung được quy định tại các khoản 1, 2, 3 và 4 Điều này và các thông tin khác được quy định tại khoản 1 Điều 8 của Luật này.

8. Tổ chức, cá nhân soạn thảo, đăng tải, tán phát thông tin trên không gian mạng có nội dung được quy định tại khoản 1, 2, 3 và 4 Điều này và các thông tin khác được quy định tại khoản 1 Điều 8 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 pháp lý theo quy định của pháp luật.

Điều 16. Phòng, chống gián điệp mạng, bảo vệ thông tin bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng

1. Hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng, bao gồm:

a) Cố ý làm lộ, chiếm đoạt, mua bán, thu giữ thông tin thuộc bí mật nhà nước, bí mật công tác; chiếm đoạt, trộm cắp, thu giữ thông tin thuộc sở hữu của người khác hoặc tiết lộ thông tin đã chiếm đoạt, trộm cắp, thu giữ gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin bí mật nhà nước, bí mật công tác, thông tin thuộc sở hữu của người khác được truyền đưa, lưu trữ trên không gian mạng;

c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa các biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, thông tin thuộc sở hữu của người khác;

d) Cố ý nghe, ghi âm cuộc đàm thoại trái phép;

đ) Hành vi khác xâm phạm bí mật nhà nước, bí mật công tác, thông tin thuộc sở hữu của người khác hoặc hình thức trao đổi thông tin riêng tư của người khác.

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

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

b) Triển khai các 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 cá nhân và kịp thời gỡ bỏ thông tin, tài liệu có nội dung thuộc danh mục bí mật nhà nước hoặc thông tin xâm phạm bí mật cá nhân trên hệ thống thông tin quản lý;

c) Phối hợp, thực hiện các yêu cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin, tài liệu có nội dung thuộc danh mục bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng.

3. Cơ quan soạn thảo, lưu trữ thông tin, tài liệu 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:

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

b) Kiểm tra an ninh mạng theo thẩm quyền đối với các 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 tại hệ thống thông tin quan trọng về an ninh quốc gia;

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

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

đ) Tham gia nghiên cứu, sản xuất các sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc danh mục bí mật nhà nước; các 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, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;

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 cán bộ, nhân viên phụ trách công nghệ thông tin tại các cơ quan nhà nước, hệ thống thông tin quan trọng về an ninh quốc gia.

5. Bộ Quốc phòng có trách nhiệm thực hiện các 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 tổ chức thực hiện pháp luật về sử dụng mật mã để bảo vệ thông tin bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

Điều 17. Phòng ngừa, xử lý hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh, trật tự

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

a) Hành vi đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3 và 4 Điều 15 và hành vi quy định tại khoản 1 Điều 16 của Luật này;

b) Tuyên truyền, kích động chiến tranh xâm lược, khủng bố, phá hoại; kích động, lôi kéo, tụ tập nhiều người phá rối an ninh, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức; tuyên truyền văn hóa phẩm đồi trụy; xúi giục, lôi kéo, kích động người khác phạm tội;

c) Xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát, uy hiếp hoặc gây thiệt hại về tinh thần của người khác; tiết lộ hoặc cố ý sử dụng các thông tin đã chiếm đoạt, làm ảnh hưởng đến danh dự, uy tín, nhân phẩm, lợi ích hợp pháp của người khác; đưa lên không gian mạng những thông tin thuộc sở hữu của người khác trái quy định của pháp luật;

d) Kinh doanh đa cấp, giao dịch tài sản, huy động vốn, trò chơi cho nhận, quy đổi, đầu tư ủy thác trái phép trên không gian mạng; mua bán, trao đổi, tặng, cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin đó; mua bán tiền giả, bằng cấp giả, chứng chỉ giả qua mạng;

đ) 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;

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 hoặc thông tin tài khoản ngân hàng khác của người khác; phát hành, cung cấp, sử dụng các phương tiện thanh toán trái phép;

g) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;

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

h) Hành vi khác sử dụng không gian mạng vi phạm pháp luật về an ninh, trật tự.

2. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm phòng, chống hành vi vi phạm pháp luật về an ninh, trật tự trên không gian mạng; thu thập, phối hợp thu thập chứng cứ từ nguồn dữ liệu điện tử theo quy định của pháp luật.

3. Việc xử lý hành vi vi phạm hành chính về an ninh mạng thực hiện theo quy định của pháp luật về xử lý vi phạm hành chính. Chính phủ quy định chi tiết việc xử lý hành vi vi phạm hành chính về an ninh mạng.

4. Việc điều tra, truy tố, xét xử tội phạm có liên quan đến không gian mạng, công nghệ thông tin, phương tiện điện tử được thực hiện theo quy định của Bộ luật Hình sự, Bộ luật Tố tụng hình sự và các quy định khác của pháp luật có liên quan.

Điều 18. Phòng, chống tấn công mạng

1. Hành vi tấn công mạng hoặc có liên quan đến tấn công mạng, bao gồm:

a) Phát tán các chương trình tin học gây hại cho mạng internet, mạng máy tính, mạng viễn thông, 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 tải dữ liệu của mạng viễn thông, mạng internet, hệ thống máy tính, phương tiện điện tử;

c) xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền tải qua mạng internet, mạng máy tính, mạng viễn thông, phương tiện điện tử;

d) xâm nhập, tạo ra hoặc khai thác các 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 tấn công mạng internet, mạng máy tính, mạng viễn thông, phương tiện điện tử để sử dụng vào mục đích trái pháp luật;

e) Các hành vi khác gây ảnh hưởng tới hoạt động bình thường của mạng internet, mạng máy tính, mạng viễn thông, phương tiện điện tử.

2. Chủ quản hệ thống thông tin có trách nhiệm áp dụng các biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi tấn công mạng vào hệ thống thông tin do thuộc phạm vi quản lý.

3. Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm đến chủ quyền, lợi ích, an ninh quốc gia, 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 các tổ chức, cá nhân có liên quan áp dụng các biện pháp xác định nguồn gốc tấn công mạng thu thập chứng cứ; yêu cầu các cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet chặn lọc thông tin nhằm ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

4. Bộ Công an chủ trì, phối hợp với bộ, ngành liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi tấn công mạng xâm phạm hoặc đe dọa xâm phạm đến chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội trên phạm vi cả nước, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ. Bộ Quốc phòng chủ trì, phối hợp với các bộ, ngành thực hiện công tác phòng ngừa phát hiện, xử lý hành vi tấn công mạng đối với hệ thống thông tin quân sự. Ban Cơ yếu Chính phủ chủ trì, phối hợp với các bộ, ngành thực hiện công tác phòng ngừa phát hiện, xử lý hành vi tấn công mạng 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, chủ quản hệ thống thông tin áp dụng tất cả các biện pháp được pháp luật quy định để phòng, chống khủng bố mạng.

2. Cơ quan, tổ chức, cá nhân căn cứ nhiệm vụ của mình thường xuyên rà soát, kiểm tra an ninh mạng 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 chuyên trách bảo vệ an ninh mạng hoặc cơ quan công an nơi gần nhất. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời trao đổi lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền theo định tại khoản 5 Điều này.

4. Cơ quan nhà nước có thẩm quyền áp dụng các biện pháp theo quy định của Luật này, Điều 29 Luật An toàn thông tin mạng và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng.

5. Bộ Công an chủ trì, phối hợp với các bộ, ngành 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 hệ thống thông tin quân sự do Bộ Quốc phòng quản lý và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; Bộ Quốc phòng chủ trì, phối hợp với các bộ, ngành triển khai công tác phòng, chống khủng bố mạng, áp dụng các biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự; Ban Cơ yếu Chính phủ chủ trì, phối hợp với các bộ, ngành triển khai công tác phòng, chống khủng bố mạng, áp dụng các biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 20. Phòng, chống chiến tranh mạng

1. Phòng, chống chiến tranh mạng là trách nhiệm của hệ thống chính trị và toàn xã hội, Nhà nước huy động mọi lực lượng tham gia phòng, chống chiến tranh mạng.

2. Bộ Quốc phòng chủ trì phòng, chống chiến tranh mạng.

Điều 21. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

1. Tình huống nguy hiểm về an ninh mạng gồm:

a) Xuất hiện thông tin kích động 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 nhập hệ thống thông tin, phương tiện điện tử gây ảnh hưởng nghiêm trọng tới chủ quyền, lợi ích, an ninh quốc gia, đặc biệt

ng nghiêm trọng tới trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc gây thiệt hại về tính mạng con người.

2. Phòng ngừa tình huống nguy hiểm về an ninh mạng:

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) Các doanh nghiệp viễn thông, internet, công nghệ thông tin, cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet và cơ quan, tổ chức, cá nhân liên quan có trách nhiệm phối hợp với 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:

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 tới 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 các khu vực cụ thể;

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

g) Thực hiện biện pháp khác theo quy định của pháp luật.

4. Thẩm quyền xử lý tình huống nguy hiểm về an ninh mạng:

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) Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể; 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 các cơ quan, tổ chức, cá nhân 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 trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện các biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

Điều 22. Đấu tranh bảo vệ an ninh mạng

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

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

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

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

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

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

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

Chương IV

TRIỂN KHAI 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 ở trung ương và địa phương

1. Nghiên cứu, ứng dụng, triển khai các 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 do mình quản lý.

2. Đào tạo, bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động và nâng cao năng lực bảo vệ an ninh mạng cho đội ngũ làm công tác bảo vệ an ninh mạng.

3. 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 cứu khẩn cấp sự cố an ninh mạng.

4. Quy hoạch, thiết kế, xây dựng mô hình mạng bảo đảm an ninh mạng.

5. Bảo vệ an ninh mạng trong các hoạt động: Cung cấp dịch vụ công trên môi trường mạng; cung cấp, trao đổi, thu thập thông tin với tổ chức, cá nhân; chia sẻ thông tin trong nội bộ và với cơ quan khác của nhà nước hoặc trong các hoạt động khác theo quy định của Chính phủ.

6. Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ hệ thống mạng.

7. Tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống tấn công mạng; ứng phó, khắc phục sự cố an ninh mạng.

8. Người đứng đầu cơ quan, tổ chức chịu trách nhiệm về việc triển khai hoạt động bảo vệ an ninh mạng thuộc thẩm quyền quản lý của mình.

Điều 24. Kiểm tra an ninh mạng đối với hệ thống thông tin của các cơ quan, tổ chức

1. Việc kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thực hiện theo quy định tại Điều 12 của Luật này. Việc kiểm tra an ninh mạng đối với hệ thống thông tin không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia thực hiện theo quy định của Điều này.

2. 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 khi có hành vi vi phạm pháp luật về an ninh mạng hoặc khi có yêu cầu quản lý nhà nước về an ninh mạng.

3. Đối tượng kiểm tra an ninh mạng áp dụng theo quy định tại khoản 3 Điều 12 của Luật này.

4. 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 do mình quản lý.

5. Trình tự, thủ tục kiểm tra an ninh mạng thực hiện theo quy định tại điểm a và điểm b khoản 5 Điều 12 của Luật này.

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

Điều 25. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế

1. Công 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.

2. Triển khai bảo vệ an ninh mạng đối với toàn bộ cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế thực hiện theo các nguyên tắc sau:

a) Kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu xây dựng, phát triển kinh tế - xã hội đối với toàn bộ cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế;

b) Khuyến khích công kết nối quốc tế đặt trên lãnh thổ Việt Nam;

c) Khuyến khích tổ chức, cá nhân cùng đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

3. Tổ chức, cá nhân có trách nhiệm bảo vệ an ninh mạng theo thẩm quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của các cơ quan nhà nước có thẩm quyền.

4. Tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, công kết nối mạng quốc tế có trách nhiệm tạo điều kiện làm việc, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để các cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ kiểm soát và bảo đảm an ninh mạng khi có yêu cầu.

Điều 26. Bảo đảm an ninh thông tin trên không gian mạng

1. Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin có nội dung quy định tại khoản 1 Điều 8 của Luật này và các thông tin khác có nội dung xâm phạm chủ quyền, an ninh quốc gia.

2. Cơ quan, tổ chức trong và ngoài nước khi cung cấp dịch vụ trên không gian mạng hoặc sở hữu hệ thống thông tin tại Việt Nam phải:

a) Thiết lập cơ chế xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản;

b) Xóa bỏ thông tin, ngăn chặn việc chia sẻ thông tin có nội dung quy định tại các khoản 1, 2, 3 và 4 Điều 15 của Luật này trên dịch vụ hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ

Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông; lưu vết liên quan để cung cấp cho lực lượng chuyên trách bảo vệ an ninh mạng;

c) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung quy định tại các khoản 1, 2, 3 và 4 Điều 15 của Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông;

d) Lưu trữ tại Việt Nam đối với thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam và các dữ liệu quan trọng liên quan đến an ninh quốc gia; đặt trụ sở hoặc văn phòng đại diện tại Việt Nam;

đ) Thực hiện yêu cầu của cơ quan chức năng trong điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng.

3. Chính phủ quy định cụ thể các loại thông tin phải lưu trữ tại Việt Nam và các cơ quan, tổ chức cung cấp dịch vụ trên không gian mạng phải đặt trụ sở hoặc văn phòng đại diện tại Việt Nam tại điểm d khoản 2 Điều này.

Điều 27. 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, hạn chế tối đa việc tồn tại lỗ hổng bảo mật và 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, quyền riêng tư cá nhân, khả năng truyền tải bảo mật của thông tin trên không gian mạng;

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

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

g) Các sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng;

h) Dự báo an ninh mạng;

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

2. Các bộ, ngành, cơ sở nghiên cứu, đào tạo và các tổ chức, cá nhân có liên quan được phép nghiên cứu, phát triển an ninh mạng; xây dựng thao trường mạng tạo môi trường thử nghiệm an ninh mạng để mô hình hóa các cuộc tấn công mạng, các phương thức phòng thủ trong môi trường và hệ thống mạng thế giới thực.

3. Chính phủ ban hành Chiến lược nghiên cứu, phát triển và bảo vệ an ninh mạng và định kỳ 05 năm một lần tiến hành rà soát để điều chỉnh cho phù hợp với công tác bảo vệ an ninh mạng, sự phát triển của khoa học công nghệ và thực tế tình hình an ninh mạng. Các bộ, ngành, chủ quản hệ thống thông tin quan trọng về an ninh quốc gia căn cứ Chiến lược nghiên cứu, phát triển và bảo vệ an ninh mạng của Chính phủ, xây dựng chiến lược hoặc kế hoạch bảo vệ an ninh mạng đối với bộ, ngành, hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 28. Nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng

1. Nhà nước khuyến khích tổ chức, cá nhân tham gia nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; ưu tiên nghiên cứu, phát triển công nghệ, sản phẩm theo quy định của Chính phủ.

2. Các chương trình, đề tài nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng được sử dụng ngân sách nhà nước; ưu tiên phát triển các mô hình gắn kết nghiên cứu, đào tạo với sản xuất sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng.

3. Việc tổ chức thực hiện các chương trình, đề tài nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng thực hiện theo quy định của pháp luật về khoa học và công nghệ.

Điều 29. Nâng cao năng lực tự chủ về an ninh mạng

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

2. Chính phủ triển khai các biện pháp nâng cao năng lực tự chủ về an ninh mạng cho các cơ quan, tổ chức, bao gồm:

a) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển các sản phẩm, dịch vụ an ninh mạng;

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

c) Đào tạo, phát triển và tuyển dụng nhân lực an ninh mạng;

d) Tăng cường môi trường và hỗ trợ các doanh nghiệp an ninh mạng phát triển mới thông qua cải thiện các điều kiện cạnh tranh;

đ) Tham gia các điều ước quốc tế về an ninh mạng trên cơ sở công nhận lẫn nhau.

Điều 30. Bảo vệ trẻ em trên không gian mạng

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

2. Chủ quản hệ thống thông tin, cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do cơ quan, tổ chức cung cấp, không để gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; tiến hành ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

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

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

Chương V

BẢO ĐẢM HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Điều 31. Lực lượng bảo vệ an ninh mạng

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

2. Lực lượng bảo vệ an ninh mạng được bố trí tại bộ, ngành, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương, chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

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

Điều 32. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng

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

2. Nhà nước có chính sách, kế hoạch xây dựng, bồi dưỡng, phát triển nguồn nhân lực bảo vệ an ninh mạng.

3. Khi xảy ra tình huống nguy hiểm về an ninh mạng, Nhà nước quyết định huy động nhân lực bảo vệ an ninh mạng theo quy định của pháp luật.

Điều 33. Đào tạo, phát triển lực lượng bảo vệ an ninh mạng

1. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng chất lượng cao, có phẩm chất đạo đức tốt.
2. Ưu tiên phát triển các 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 tư nhân, trong và ngoài nước.

Điều 34. Giáo dục, bồi dưỡng kiến thức về an ninh mạng

1. Giáo dục an ninh mạng được đưa vào môn học chính khóa về giáo dục quốc phòng, an ninh trong nhà trường; bồi dưỡng kiến thức về an ninh mạng được đưa vào chương trình khung bồi dưỡng kiến thức quốc phòng, an ninh theo quy định của Luật Giáo dục quốc phòng, an ninh.
2. Bộ Quốc phòng chủ trì, phối hợp với Bộ Công an, Bộ Giáo dục và Đào tạo, bộ, cơ quan ngang bộ, cơ quan, tổ chức ở trung ương có liên quan đưa nội dung giáo dục an ninh mạng vào chương trình khung giáo dục quốc phòng và an ninh cho người học trong trường của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội; chương trình, nội dung bồi dưỡng kiến thức quốc phòng và an ninh cho đối tượng trong cơ quan, tổ chức của Nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội, doanh nghiệp ngoài khu vực nhà nước, đơn vị sự nghiệp ngoài công lập.
3. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, các bộ, ngành có liên quan tổ chức bồi dưỡng kiến thức an ninh mạng cho cán bộ chuyên trách bảo vệ an ninh mạng và cán bộ, công chức, viên chức tham gia bảo vệ an ninh mạng.

Điều 35. Phổ biến kiến thức về an ninh mạng

1. Nhà nước có chính sách phổ biến kiến thức an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với các tổ chức tư nhân, cá nhân thực hiện các chương trình giáo dục và nâng cao nhận thức về an ninh mạng.
2. Bộ Công an chủ trì, phối hợp với các bộ, ngành, cơ quan, tổ chức xây dựng và triển khai các hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong cơ quan, tổ chức.
3. Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương có trách nhiệm xây dựng và triển khai các hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho tổ chức, cá nhân trong địa phương mình.

Điều 36. Bảo đảm trang thiết bị, cơ sở vật chất phục vụ triển khai hoạt động bảo vệ an ninh mạng

Nhà nước bảo đảm trang thiết bị, cơ sở vật chất phục vụ triển khai hoạt động bảo vệ an ninh mạng phù hợp với yêu cầu phát triển kinh tế - xã hội và tình hình an ninh mạng; huy động cơ sở hạ tầng không gian mạng của các cơ quan, tổ chức trong trường hợp cần thiết theo quy định của pháp luật.

Điều 37. Kinh phí bảo đảm hoạt động bảo vệ an ninh mạng

1. Kinh phí thực hiện hoạt động bảo vệ an ninh mạng của các cơ quan nhà nước do ngân sách nhà nước bảo đảm, được sử dụng trong dự toán ngân sách nhà nước hằng năm theo quy định của pháp luật về phân cấp ngân sách nhà nước. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật.

2. Kinh phí thực hiện hoạt động bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan, tổ chức ngoài cơ quan nhà nước do cơ quan, tổ chức tự bảo đảm.

3. Bộ Tài chính, Bộ Kế hoạch và Đầu tư, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương có trách nhiệm bố trí kinh phí cho hoạt động bảo vệ an ninh mạng của các cơ quan nhà nước theo quy định của pháp luật.

Chương VI

TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

Điều 38. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng

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

2. Kịp thời cung cấp những 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 quản lý nhà nước có thẩm quyền, lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Công an hoặc cơ quan công an nơi gần nhất.

3. Thực hiện yêu cầu và hướng dẫn của cơ quan quản lý nhà nước 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.

Điều 39. Trách nhiệm của chủ thể cung cấp thiết bị số, dịch vụ mạng, ứng dụng mạng

1. Cảnh báo về khả năng, tình huống có khả năng mất an ninh mạng của thiết bị số, dịch vụ mạng, ứng dụng mạng và hướng dẫn biện pháp phòng ngừa.

2. Tạm ngừng hoặc ngừng cung cấp thiết bị số, dịch vụ mạng, ứng dụng mạng đối với tổ chức, cá nhân trong phạm vi không gian, thời gian nhất định khi có yêu cầu của cơ quan nhà nước có thẩm quyền để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội.

3. Phối hợp với cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nhằm xác minh thông tin, xác định chủ thể đăng ký sử dụng tài khoản số.

Điều 40. Trách nhiệm của cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet

1. Yêu cầu chủ thể sử dụng cung cấp thông tin xác thực.

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

3. Hợp tác, cung cấp các biện pháp kỹ thuật, hỗ trợ cơ quan chức năng trong quá trình điều tra tội phạm và bảo vệ an ninh quốc gia theo quy định của pháp luật.

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

5. Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong hoạt động bảo vệ an ninh mạng.

6. Thực hiện quy định tại khoản 2 Điều 26 của Luật này.

7. Chính phủ quy định cụ thể về xử lý vi phạm các quy định về bảo vệ an ninh mạng của các cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet.

Điều 41. Trách nhiệm của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia

1. Xây dựng quy chế vận hành, bảo vệ an ninh mạng, áp dụng các biện pháp tương ứng đối với hệ thống thông tin do mình quản lý; lập phương án phòng ngừa, ứng phó, khắc phục sự cố an ninh mạng.

2. Kiểm tra, giám sát, ứng phó, khắc phục sự cố về an ninh mạng theo quy định của Luật này.

3. Bảo đảm hệ thống thông tin quan trọng về an ninh quốc gia đáp ứng điều kiện an ninh mạng.

4. Khi thu thập, tạo ra thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam, các dữ liệu quan trọng liên quan đến an ninh quốc gia theo quy định tại điểm d khoản 2 Điều 26 của Luật này phải lưu trữ tại Việt Nam. Trong trường hợp cần thiết phải cung cấp thông tin trên ra ngoài lãnh thổ quốc gia thực hiện theo quy định của pháp luật và hướng dẫn của Bộ trưởng Bộ Công an.

5. Phối hợp với Bộ Công an hoặc tổ chức chuyên môn do Bộ Công an chỉ định kiểm tra an ninh mạng trước khi đưa vào vận hành, khai thác các thiết bị phục vụ hệ thống thông tin quan trọng về an ninh quốc gia; có phương án bảo vệ an ninh mạng trước khi thiết lập, mở rộng, nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

6. Định kỳ phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tổ chức tập huấn, bồi dưỡng về kiến thức, kỹ thuật và đánh giá kỹ năng an ninh mạng cho các nhân viên phụ trách bảo vệ an ninh mạng của hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 42. Trách nhiệm của Bộ Công an

1. Chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng:

a) Thực hiện quản lý nhà nước về bảo vệ an ninh mạng đối với hệ thống thông tin, phương tiện điện tử, dịch vụ mạng, ứng dụng mạng;

b) Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành các văn bản quy phạm pháp luật về an ninh mạng; tuyên truyền, phổ biến pháp luật về an ninh mạng.

c) Chủ trì, phối hợp với các bộ, ngành trình Thủ tướng Chính phủ ban hành Danh mục hệ thống thông tin quan trọng về an ninh quốc gia và quy định cơ chế phối hợp giữa các bộ trong thực hiện các nội dung quản lý nhà nước có liên quan đối với hệ thống thông tin quan trọng về an ninh quốc gia.

d) Thẩm định, kiểm tra, giám sát, đánh giá điều kiện, ứng phó, khắc phục sự cố về an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo quy định của Luật này;

đ) Quản lý nhà nước về an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối quốc tế; quản lý hoạt động bảo vệ an ninh mạng của các cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet;

e) Quản lý nhà nước về giám sát an ninh mạng; cảnh báo, chia sẻ thông tin an ninh mạng, các nguy cơ đe dọa an ninh mạng.

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

3. 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.

4. Bảo đảm an ninh thông tin mạng; xây dựng cơ chế xác thực thông tin đăng ký tài khoản số; ngăn chặn, xử lý thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân, trái đạo đức, thuần phong mỹ tục trên không gian mạng.

5. Huy động tổ chức, cá nhân tham gia bảo vệ an ninh mạng; huy động nhân lực, cơ sở hạ tầng không gian mạng thuộc bộ, ngành, địa phương, doanh nghiệp viễn thông, internet, công nghệ thông tin khi xảy ra tình huống nguy hiểm về an ninh mạng theo quy định của pháp luật.

6. Bảo vệ bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng.

7. Phòng, chống tấn công mạng, khủng bố mạng, gián điệp mạng, chủ trì xử lý tình huống nguy hiểm về an ninh mạng; chủ trì thực hiện đấu tranh bảo vệ an ninh mạng và tham gia phòng, chống chiến tranh mạng.

8. 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.

9. Phối hợp với các bộ, ngành liên quan trong đào tạo, phát triển nguồn nhân lực an ninh mạng.

10. Xử lý các hành vi vi phạm pháp luật về an ninh mạng theo quy định của pháp luật.

11. Chủ trì hợp tác quốc tế về an ninh mạng.

Điều 43. Trách nhiệm của Bộ Quốc phòng

1. Chịu trách nhiệm trước Chính phủ quản lý nhà nước về nhiệm vụ quân sự, quốc phòng trên không gian mạng.

a) Thực hiện quản lý nhà nước về nhiệm vụ quân sự, quốc phòng trên không gian mạng.

b) Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong thực hiện nhiệm vụ quốc phòng trên không gian mạng.

c) Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành các văn bản quy phạm pháp luật về thực hiện nhiệm vụ quốc phòng trên không gian mạng.

d) Thẩm định, kiểm tra, giám sát, đánh giá điều kiện, ứng phó, khắc phục sự cố về an ninh mạng đối với hệ thống thông tin quân sự theo quy định của Luật này.

đ) Bảo vệ bí mật quân sự, bí mật nhà nước trên hệ thống thông tin quân sự theo chức năng, nhiệm vụ được giao; phòng ngừa, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quân đội.

2. Chủ trì rà soát hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Bộ Công an trình Thủ tướng Chính phủ ban hành Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. 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, quản lý nhà nước về an ninh mạng theo chức năng, nhiệm vụ được giao; đưa kiến thức an ninh mạng vào chương trình giáo dục quốc phòng, an ninh.

4. Hợp tác quốc tế về an ninh mạng theo chức năng, nhiệm vụ được giao.

Điều 44. Trách nhiệm của Bộ Thông tin và Truyền thông

1. Phối hợp với Bộ Công an, Bộ Quốc phòng trong bảo vệ an ninh mạng.

2. 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 16 của Luật này.

3. Yêu cầu cơ quan, tổ chức cung cấp dịch vụ trên mạng viễn thông, mạng internet, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của tổ chức, cá nhân, thông tin có nội dung trái đạo đức, thuần phong mỹ tục và thông tin vi

phạm phạm pháp luật khác trên dịch vụ, hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý.

4. Xử lý các hành vi vi phạm pháp luật về an ninh mạng theo quy định của pháp luật.

Điều 45. Trách nhiệm của Ban Cơ yếu Chính phủ

1. Làm lực lượng nòng cốt, chuyên trách trong quản lý, sử dụng nghiệp vụ mật mã, kỹ thuật mật mã và các giải pháp có liên quan đến mật mã để bảo vệ thông tin bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

2. Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành chiến lược, chính sách, văn bản quy phạm pháp luật về mật mã để bảo vệ thông tin bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

3. Giúp Bộ trưởng Bộ Quốc phòng tổ chức thực hiện chiến lược, chính sách, pháp luật về mật mã để bảo vệ thông tin bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

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

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

Điều 46. Trách nhiệm của bộ, ngành, ủy ban nhân dân cấp tỉnh, thành phố trực thuộc Trung ương

Trong phạm vi, nhiệm vụ, quyền hạn của mình có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin do mình quản lý và phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng ở bộ, ngành, ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương.

Chương VII

ĐIỀU KHOẢN THI HÀNH

Điều 47. Hiệu lực thi hành

1. Luật này có hiệu lực thi hành từ ngày tháng năm 2018.

2. Hệ thống thông tin đã vận hành, sử dụng phải được tiến hành kiểm tra an ninh mạng, giám sát an ninh mạng trong thời hạn 06 tháng và bổ sung đầy đủ

các điều kiện an ninh mạng trong thời hạn 36 tháng kể từ ngày được đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia có hiệu lực thi hành.

Luật này đã được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ thông qua ngày tháng năm 2018.