CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 343/2026/NĐ-CP	*Hà Nội, ngày 03 tháng 9 năm 2026*

NGHỊ ĐỊNH
Quy định chi tiết một số điều của Luật An ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng và ngăn chặn xung đột thông tin trên không gian mạng

Căn cứ Luật Tổ chức Chính phủ số 63/2025/QH15;

Căn cứ Luật An ninh quốc gia số 32/2004/QH11;

Căn cứ Luật Quốc phòng số 22/2018/QH14;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Theo đề nghị của Bộ trưởng Bộ Quốc phòng;

Chính phủ ban hành Nghị định quy định chi tiết một số điều của Luật An ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng và ngăn chặn xung đột thông tin trên không gian mạng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Nghị định này quy định chi tiết một số điều của Luật An ninh mạng, gồm:

a) Điểm a, b, c, d, đ, e, g, h, i, k, l, m khoản 1 Điều 5, khoản 2 Điều 8, khoản 5 Điều 9, khoản 6 Điều 10, khoản 5 Điều 12, khoản 5 Điều 14, khoản 4 Điều 25, khoản 3 Điều 26, khoản 3 Điều 28, khoản 3 Điều 29, khoản 2 Điều 30, khoản 5 Điều 34 thuộc phạm vi quản lý của Bộ Quốc phòng;

b) Khoản 4 Điều 22 về ngăn chặn xung đột thông tin trên không gian mạng.

2. Những nội dung chưa được quy định tại Nghị định này thì thực hiện theo quy định của pháp luật về an ninh mạng và pháp luật có liên quan.

Điều 2. Đối tượng áp dụng

1. Nghị định này áp dụng đối với cơ quan, đơn vị, tổ chức, doanh nghiệp, cá nhân thuộc phạm vi quản lý của Bộ Quốc phòng và các chủ thể có liên quan đến việc thực hiện các nội dung quy định tại điểm a khoản 1 Điều 1 Nghị định này.

2. Nghị định này áp dụng đối với cơ quan, tổ chức, doanh nghiệp, cá nhân có liên quan đến việc thực hiện các nội dung quy định tại điểm b khoản 1 Điều 1 Nghị định này.

Điều 3. Giải thích từ ngữ

Trong Nghị định này, từ ngữ dưới đây được hiểu như sau:

Biện pháp nghiệp vụ bảo vệ an ninh mạng trong Nghị định này là các biện pháp quy định tại các điểm e, h, i, k, m khoản 1 Điều 5 Luật An ninh mạng, được áp dụng trong phạm vi quản lý của Bộ Quốc phòng theo quy định của pháp luật.

Điều 4. Nguyên tắc bảo vệ an ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng và ngăn chặn xung đột thông tin trên không gian mạng

1. Bộ Quốc phòng quản lý về an ninh mạng đối với nhiệm vụ quân sự, quốc phòng. Bộ Công an quản lý về an ninh mạng đối với các đơn vị Quân đội có hoạt động dân sự, kinh tế theo thẩm quyền. Đối với các nội dung giao thoa, hai Bộ thống nhất quy chế phối hợp.

2. Việc áp dụng các biện pháp bảo vệ an ninh mạng theo Nghị định này thực hiện trong phạm vi chức năng, nhiệm vụ, quyền hạn của Bộ Quốc phòng và đối với hệ thống thông tin quân sự, các nội dung thuộc phạm vi quản lý của Bộ Quốc phòng theo quy định của pháp luật.

3. Bộ Quốc phòng thống nhất tổ chức thực hiện nhiệm vụ, biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin quân sự theo quy định của pháp luật về an ninh mạng và pháp luật có liên quan; phát huy vai trò của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.

4. Việc kết nối, cung cấp, chia sẻ thông tin, tài liệu phục vụ bảo vệ an ninh mạng phải bảo đảm yêu cầu bảo vệ bí mật nhà nước và không làm ảnh hưởng đến việc thực hiện nhiệm vụ thuộc phạm vi quản lý của Bộ Quốc phòng.

5. Việc bảo đảm an ninh dữ liệu trong lĩnh vực quân sự, quốc phòng phải được thực hiện xuyên suốt trong toàn bộ vòng đời dữ liệu; áp dụng biện pháp quản lý và biện pháp kỹ thuật phù hợp với mức độ phân loại dữ liệu, cấp độ hệ thống thông tin quân sự và yêu cầu nhiệm vụ quân sự, quốc phòng.

6. Chủ động phòng ngừa, ngăn chặn xung đột thông tin trên không gian mạng; kịp thời phát hiện, xử lý các nguy cơ đe dọa an ninh mạng, không để xảy ra chiến tranh thông tin, chiến tranh không gian mạng dưới mọi hình thức.

7. Nghiêm cấm lợi dụng, lạm dụng các biện pháp bảo vệ an ninh mạng để xâm phạm quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc thực hiện hành vi vi phạm pháp luật; tổ chức, cá nhân vi phạm tùy theo tính chất, mức độ vi phạm bị xử lý theo quy định của pháp luật.

Điều 5. Lực lượng bảo vệ an ninh mạng và huy động lực lượng bảo vệ an ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng

1. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng gồm Cục Bảo vệ an ninh Quân đội thuộc Tổng cục Chính trị Quân đội nhân dân Việt Nam và Bộ Tư lệnh Tác chiến không gian mạng.

2. Trường hợp cần thiết để xử lý sự cố an ninh mạng, tấn công mạng hoặc tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự, Bộ Quốc phòng chủ trì, phối hợp với cơ quan, tổ chức có liên quan huy động lực lượng, phương tiện theo quy định của pháp luật.

Điều 6. Hoạt động tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng thuộc phạm vi quản lý của Bộ Quốc phòng

1. Nội dung về chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng; chương trình, nội dung, việc chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng thực hiện theo quy định của pháp luật về an ninh mạng.

2. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng và các cơ quan, đơn vị, doanh nghiệp thuộc Bộ Quốc phòng đáp ứng đầy đủ các điều kiện theo quy định của pháp luật về an ninh mạng được tổ chức hoạt động tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng cho các đối tượng thuộc phạm vi quản lý của Bộ Quốc phòng.

3. Cơ quan, đơn vị, doanh nghiệp thuộc Bộ Quốc phòng được tổ chức hoạt động tập huấn có trách nhiệm gửi thông tin về chứng nhận đã cấp đến Bộ Tư lệnh Tác chiến không gian mạng để cập nhật, quản lý theo quy định.

4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng chịu trách nhiệm xây dựng, quản lý cơ sở dữ liệu về học viên, giảng viên tập huấn an ninh mạng và chứng nhận, chứng chỉ chuyên môn.

5. Bộ Quốc phòng ban hành khung chương trình đào tạo, tập huấn tương ứng với từng chuẩn kiến thức, kỹ năng nền tảng và chuẩn kỹ năng chuyên sâu về an ninh mạng làm căn cứ thống nhất để tổ chức tập huấn, đánh giá kết quả và cấp chứng nhận; hướng dẫn về chương trình, nội dung tập huấn; tiêu chuẩn, quy trình đánh giá kết quả học tập; mẫu chứng nhận tập huấn; thực hiện kiểm tra, giám sát và xử lý vi phạm trong hoạt động tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng thuộc phạm vi quản lý.

Chương II
BẢO VỆ AN NINH MẠNG, PHÒNG NGỪA, XỬ LÝ THÔNG TIN, HÀNH VI XÂM PHẠM AN NINH MẠNG, BẢO ĐẢM AN NINH THÔNG TIN MẠNG VÀ BẢO ĐẢM AN NINH DỮ LIỆU THUỘC PHẠM VI QUẢN LÝ CỦA BỘ QUỐC PHÒNG

Mục 1
BẢO VỆ AN NINH MẠNG

Điều 7. Phân loại cấp độ hệ thống thông tin quân sự

1. Các hệ thống thông tin quân sự phải xác định cấp độ và có giải pháp bảo đảm an ninh mạng tương ứng với cấp độ.

2. Việc xác định cấp độ đối với hệ thống thông tin quân sự được thực hiện trên cơ sở quy định của pháp luật về an ninh mạng. Bộ Quốc phòng hướng dẫn tổ chức thực hiện đối với hệ thống thông tin quân sự thuộc phạm vi quản lý.

3. Thẩm quyền, trình tự, thủ tục xác định cấp độ

a) Đối với hệ thống thông tin quân sự được đề xuất cấp độ 1, cấp độ 2: Cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ Quốc phòng là chủ quản hệ thống thông tin quân sự chủ trì xây dựng, thẩm định, phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng;

b) Đối với hệ thống thông tin quân sự được đề xuất cấp độ 3: Cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ Quốc phòng lập hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng; gửi 01 bộ hồ sơ về Bộ Tư lệnh Tác chiến không gian mạng để tổ chức thẩm định. Trong thời hạn 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ, Bộ Tư lệnh Tác chiến không gian mạng chủ trì, phối hợp với các cơ quan, đơn vị liên quan thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng. Trên cơ sở kết quả thẩm định, cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ Quốc phòng phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng;

c) Đối với hệ thống thông tin quân sự được đề xuất cấp độ 4: Cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ Quốc phòng lập hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng; gửi 01 bộ hồ sơ về Bộ Tư lệnh Tác chiến không gian mạng để tổ chức thẩm định. Trong thời hạn 10 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ, Bộ Tư lệnh Tác chiến không gian mạng chủ trì phối hợp với các cơ quan chức năng của Bộ Quốc phòng thẩm định hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng; trình Bộ trưởng Bộ Quốc phòng phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng;

d) Đối với hệ thống thông tin quân sự được đề xuất cấp độ 5 (hệ thống thông tin quan trọng về an ninh quốc gia): Cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ Quốc phòng lập hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng; gửi 01 bộ hồ sơ về Bộ Tư lệnh Tác chiến không gian mạng để tổ chức thẩm định. Trong thời hạn 15 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ, Bộ Tư lệnh Tác chiến không gian mạng chủ trì, phối hợp với các cơ quan liên quan thẩm định, báo cáo Bộ trưởng Bộ Quốc phòng phê duyệt phương án bảo đảm an ninh mạng; trình Thủ tướng Chính phủ phê duyệt hệ thống thông tin quân sự cấp độ 5.

4. Cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ Quốc phòng có trách nhiệm áp dụng biện pháp, thực hiện nghĩa vụ bảo đảm an ninh mạng tương ứng với cấp độ hệ thống thông tin quân sự đã được xác định.

Điều 8. Hệ thống thông tin quân sự thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Bộ Quốc phòng chủ trì rà soát, đánh giá, lập hồ sơ đề xuất đưa hệ thống thông tin quân sự vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia hoặc đưa hệ thống thông tin quân sự ra khỏi Danh mục hệ thống thông tin quan trọng về an ninh quốc gia khi không còn đáp ứng tiêu chí theo quy định.

2. Hệ thống thông tin quân sự thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng các tiêu chí, điều kiện bảo đảm an ninh mạng theo quy định của pháp luật và được áp dụng các biện pháp bảo vệ an ninh mạng phù hợp với tính chất, yêu cầu quản lý, vận hành của hệ thống.

3. Bộ Quốc phòng hướng dẫn việc rà soát, đánh giá, lập hồ sơ đề xuất đối với hệ thống thông tin quân sự.

Điều 9. Thẩm định an ninh mạng hệ thống thông tin quân sự

1. Đối tượng thực hiện thẩm định an ninh mạng

a) Đối tượng bắt buộc thực hiện thẩm định an ninh mạng: Hệ thống thông tin quân sự thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trước khi đưa vào sử dụng hoặc khi đầu tư nâng cấp, mở rộng phải thay đổi phương án thiết kế, phương án bảo đảm an ninh mạng;

b) Hệ thống thông tin quân sự không thuộc đối tượng tại điểm a khoản 1 Điều này theo quy định của Bộ Quốc phòng.

2. Đối tượng thẩm định an ninh mạng

a) Hồ sơ thiết kế dự án đầu tư xây dựng mới hệ thống thông tin quân sự;

b) Hồ sơ thiết kế dự án đầu tư nâng cấp, mở rộng hệ thống thông tin quân sự đối với trường hợp phải thay đổi phương án thiết kế, phương án bảo đảm an ninh mạng.

3. Nội dung thẩm định an ninh mạng

a) Việc tuân thủ các quy định, điều kiện về an ninh mạng trong thiết kế hệ thống thông tin quân sự;

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

4. Bộ Tư lệnh Tác chiến không gian mạng chủ trì thực hiện thẩm định an ninh mạng đối với hệ thống thông tin quân sự.

Điều 10. Trình tự, thủ tục thẩm định an ninh mạng hệ thống thông tin quân sự

1. Trình tự thực hiện thẩm định an ninh mạng

a) Sau khi hệ thống thông tin quân sự đã được thẩm định cấp độ an ninh mạng theo quy định của pháp luật, chủ quản hệ thống thông tin quân sự nộp hồ sơ đề nghị thẩm định an ninh mạng đến Bộ Tư lệnh Tác chiến không gian mạng;

b) Bộ Tư lệnh Tác chiến không gian mạng tiếp nhận, kiểm tra hồ sơ và cấp giấy tiếp nhận trong thời hạn 03 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ;

c) Bộ Tư lệnh Tác chiến không gian mạng tổ chức nghiên cứu hồ sơ, tài liệu kỹ thuật; đánh giá thực tế hệ thống; kiểm thử, rà soát lỗ hổng bảo mật; đánh giá phương án bảo vệ, giám sát, ứng cứu sự cố an ninh mạng và thông báo kết quả thẩm định an ninh mạng trong thời hạn 10 ngày làm việc kể từ ngày cấp giấy tiếp nhận hồ sơ.

2. Hồ sơ đề nghị thẩm định an ninh mạng

a) Văn bản đề nghị thẩm định an ninh mạng;

b) Quy định, quy trình, phương án bảo đảm an ninh mạng và nhân sự bảo vệ an ninh mạng; biện pháp bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm; biện pháp kỹ thuật giám sát, bảo vệ an ninh mạng; biện pháp bảo đảm an ninh vật lý, kiểm soát truy cập, chống rò rỉ dữ liệu;

c) Tài liệu thể hiện kết quả thẩm định cấp độ an ninh mạng của hệ thống thông tin quân sự.

3. Trường hợp cần xác định sự phù hợp giữa hiện trạng của hệ thống thông tin quân sự và hồ sơ đề nghị thẩm định, cơ quan có thẩm quyền tiến hành khảo sát, đánh giá hiện trạng thực tế của hệ thống thông tin quân sự để đối chiếu với hồ sơ đề nghị thẩm định. Việc khảo sát, đánh giá thực tế bảo đảm không gây ảnh hưởng tới hoạt động bình thường của chủ quản cũng như hệ thống thông tin quân sự. Thời gian khảo sát, đánh giá thực tế không quá 07 ngày làm việc.

4. Kết quả thẩm định an ninh mạng được quản lý theo quy định của pháp luật.

Điều 11. Đánh giá điều kiện an ninh mạng hệ thống thông tin quân sự

1. Đối tượng thực hiện đánh giá điều kiện an ninh mạng

a) Đối tượng bắt buộc thực hiện đánh giá điều kiện an ninh mạng: Hệ thống thông tin quân sự thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trước khi đưa vào sử dụng hoặc khi đầu tư nâng cấp, mở rộng phải thay đổi phương án thiết kế, phương án bảo đảm an ninh mạng;

b) Hệ thống thông tin quân sự không thuộc đối tượng tại điểm a khoản 1 Điều này theo quy định của Bộ Quốc phòng.

2. Nội dung đánh giá điều kiện an ninh mạng

a) Đánh giá điều kiện về tổ chức và nhân sự bảo đảm an ninh mạng, bao gồm: Tổ chức bộ phận chuyên trách về an ninh mạng; năng lực chuyên môn của nhân sự;

b) Đánh giá điều kiện về hạ tầng kỹ thuật bảo đảm an ninh mạng, bao gồm: Hệ thống thiết bị bảo mật; hệ thống giám sát an ninh mạng; hệ thống sao lưu và khôi phục dữ liệu;

c) Đánh giá điều kiện về quy chế, quy trình bảo đảm an ninh mạng;

d) Đánh giá mức độ tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng.

3. Bộ Tư lệnh Tác chiến không gian mạng chủ trì thực hiện đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự, bao gồm:

a) Đánh giá hồ sơ, tài liệu kỹ thuật;

b) Kiểm tra, đánh giá thực tế tại hệ thống;

c) Thử nghiệm, kiểm thử, rà soát lỗ hổng, đánh giá xâm nhập;

d) Mô phỏng, diễn tập tình huống an ninh mạng (nếu cần thiết).

4. Hệ thống thông tin quân sự chỉ được đưa vào vận hành, kết nối mạng khi được chứng nhận đủ điều kiện an ninh mạng.

Điều 12. Trình tự, thủ tục đánh giá điều kiện an ninh mạng hệ thống thông tin quân sự

1. Trình tự đánh giá điều kiện an ninh mạng

a) Chủ quản hệ thống thông tin quân sự gửi hồ sơ đề nghị đánh giá điều kiện an ninh mạng đến Bộ Tư lệnh Tác chiến không gian mạng;

b) Bộ Tư lệnh Tác chiến không gian mạng tiếp nhận, kiểm tra, hướng dẫn hoàn thiện hồ sơ đề nghị đánh giá điều kiện an ninh mạng và cấp giấy tiếp nhận ngay sau khi nhận đủ hồ sơ;

c) Bộ Tư lệnh Tác chiến không gian mạng tiến hành đánh giá, cấp chứng nhận đủ điều kiện an ninh mạng trong thời hạn 10 ngày làm việc sau khi tiếp nhận đủ hồ sơ hợp lệ. Trường hợp không đủ điều kiện, trong 03 ngày làm việc phải thông báo, yêu cầu chủ quản hệ thống thông tin quân sự khắc phục và thực hiện lại quy trình đánh giá.

2. Hồ sơ đề nghị chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự

a) Văn bản đề nghị chứng nhận điều kiện an ninh mạng;

b) Báo cáo nghiên cứu tiền khả thi, báo cáo nghiên cứu khả thi, báo cáo đề xuất chủ trương đầu tư, hồ sơ thiết kế dự án đầu tư xây dựng mới, nâng cấp, mở rộng hệ thống thông tin quân sự trước khi phê duyệt;

c) Hồ sơ giải pháp bảo đảm an ninh mạng đối với hệ thống thông tin quân sự.

3. Bộ Tư lệnh Tác chiến không gian mạng tổ chức đánh giá đúng trình tự, thủ tục; bảo đảm khách quan, chính xác; giữ bí mật thông tin trong quá trình đánh giá. Cơ quan, đơn vị đề nghị đánh giá có trách nhiệm phối hợp cung cấp đầy đủ thông tin, tài liệu; bảo đảm điều kiện kỹ thuật phục vụ đánh giá; thực hiện yêu cầu của cơ quan đánh giá.

Điều 13. Giám sát an ninh mạng hệ thống thông tin quân sự

1. Hệ thống thông tin quân sự phải được thực hiện giám sát an ninh mạng phù hợp với cấp độ, tính chất, quy mô, phạm vi hoạt động và yêu cầu nhiệm vụ quân sự, quốc phòng.

2. Bộ Quốc phòng chủ trì tổ chức thực hiện hoạt động giám sát an ninh mạng hệ thống thông tin quân sự.

3. Trách nhiệm của chủ quản hệ thống thông tin quân sự

a) Tổ chức giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý;

b) Xây dựng cơ chế tự giám sát, 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;

c) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng trong tổ chức giám sát an ninh mạng.

4. Nội dung giám sát an ninh mạng

a) Theo dõi, giám sát hoạt động của hệ thống thông tin quân sự, hạ tầng mạng, thiết bị công nghệ thông tin và các thành phần liên quan;

b) Thu thập và phân tích dữ liệu nhật ký hệ thống, lưu lượng mạng và thông tin cần thiết phục vụ phát hiện nguy cơ mất an ninh mạng;

c) Phát hiện dấu hiệu tấn công mạng, xâm nhập trái phép, phát tán mã độc, hành vi gây mất an ninh mạng;

d) Giám sát lỗ hổng, điểm yếu an ninh mạng;

đ) Phân tích, đánh giá mức độ ảnh hưởng của nguy cơ, sự cố an ninh mạng;

e) Cảnh báo nguy cơ đe dọa an ninh mạng.

Điều 14. Trình tự, thủ tục, thẩm quyền giám sát an ninh mạng hệ thống thông tin quân sự

1. Trình tự, thủ tục thực hiện giám sát an ninh mạng

a) Thiết lập hệ thống kỹ thuật và cơ chế giám sát an ninh mạng;

b) Thu thập dữ liệu, thông tin phục vụ hoạt động giám sát an ninh mạng;

c) Phân tích, đánh giá dữ liệu và thông tin thu thập;

d) Xác định nguy cơ, mức độ ảnh hưởng của sự cố, hành vi xâm phạm an ninh mạng;

đ) Thực hiện cảnh báo nguy cơ, sự cố an ninh mạng đối với chủ quản hệ thống thông tin quân sự;

e) Áp dụng biện pháp cần thiết để ngăn chặn, xử lý và khắc phục nguy cơ, sự cố an ninh mạng theo quy định của pháp luật.

2. Trách nhiệm của chủ quản hệ thống thông tin quân sự

a) Tổ chức triển khai hoạt động giám sát an ninh mạng;

b) Khi phát hiện dấu hiệu tấn công mạng hoặc nguy cơ đe dọa an ninh mạng, tiến hành xác minh thông tin, đánh giá mức độ nguy cơ; thực hiện biện pháp kỹ thuật để ngăn chặn, hạn chế ảnh hưởng; thông báo cho các cơ quan, đơn vị có liên quan để phối hợp xử lý; báo cáo lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng trong trường hợp sự cố nghiêm trọng hoặc vượt quá khả năng xử lý;

c) Sau khi xử lý sự cố an ninh mạng tiến hành kiểm tra, đánh giá lại tình trạng an ninh mạng của hệ thống; khôi phục hoạt động bình thường của hệ thống thông tin; lập hồ sơ, lưu trữ thông tin liên quan đến quá trình xử lý sự cố an ninh mạng; báo cáo kết quả về lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.

3. Trách nhiệm của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng

a) Chủ trì tổ chức thực hiện giám sát an ninh mạng đối với hệ thống thông tin quân sự;

b) Chỉ đạo, hướng dẫn chủ quản hệ thống thông tin quân sự kết nối, duy trì hệ thống giám sát an ninh mạng, hệ thống phòng, chống mã độc tập trung về Bộ Tư lệnh Tác chiến không gian mạng;

c) Quyết định việc cung cấp thông tin, dữ liệu kỹ thuật cần thiết phục vụ hoạt động giám sát theo quy định của pháp luật.

4. Thông tin, dữ liệu thu thập từ hoạt động giám sát an ninh mạng được quản lý, khai thác theo pháp luật về an ninh mạng, bảo vệ bí mật nhà nước và quy định của Bộ Quốc phòng.

Điều 15. Kiểm tra an ninh mạng hệ thống thông tin quân sự

1. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng chủ trì, phối hợp với cơ quan, đơn vị liên quan tổ chức thực hiện kiểm tra an ninh mạng hệ thống thông tin quân sự.

2. Trường hợp kiểm tra an ninh mạng

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

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

c) Thực hiện định kỳ theo quy định;

d) Khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng.

3. Đối tượng kiểm tra an ninh mạng

a) Hệ thống phần cứng, phần mềm, thiết bị số;

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

c) Thông tin lưu trữ, xử lý, truyền đưa;

d) Phương án ứng phó, khắc phục sự cố;

đ) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất dữ liệu;

e) Hồ sơ nhân lực.

4. Nội dung kiểm tra an ninh mạng

a) Việc tuân thủ pháp luật về an ninh mạng, bảo vệ bí mật nhà nước;

b) Triển khai, duy trì và hiệu quả của các phương án, biện pháp bảo đảm an ninh mạng, phương án, kế hoạch ứng phó và khắc phục sự cố an ninh mạng;

c) Công tác phát hiện, đánh giá điểm yếu, lỗ hổng bảo mật, mã độc và thử nghiệm khả năng xâm nhập hệ thống thông tin quân sự khi cần thiết;

d) Nội dung kiểm tra khác theo quyết định của cơ quan kiểm tra hoặc đề nghị của chủ quản hệ thống thông tin quân sự.

5. Chủ quản hệ thống thông tin quân sự có trách nhiệm cung cấp thông tin, tài liệu, thực hiện các yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng để phục vụ hoạt động kiểm tra an ninh mạng.

Điều 16. Trình tự, thủ tục kiểm tra an ninh mạng hệ thống thông tin quân sự

1. Trình tự, thủ tục kiểm tra an ninh mạng

a) Thông báo kế hoạch hoặc quyết định kiểm tra an ninh mạng, trừ trường hợp kiểm tra đột xuất nhằm ngăn chặn kịp thời nguy cơ xâm hại an ninh quốc gia, an ninh quân đội;

b) Tiến hành kiểm tra an ninh mạng, bảo đảm phối hợp với chủ quản hệ thống thông tin quân sự và không làm gián đoạn hoạt động bình thường của hệ thống, trừ trường hợp cần thiết để bảo vệ an ninh quốc gia, an ninh quân đội;

c) Lập biên bản về quá trình và kết quả kiểm tra an ninh mạng, quản lý và bảo quản theo quy định;

d) Thông báo kết quả kiểm tra an ninh mạng.

2. Trường hợp cần giữ nguyên hiện trạng hệ thống thông tin quân sự để phục vụ điều tra, xử lý vi phạm pháp luật, xác minh sự cố an ninh mạng hoặc khắc phục điểm yếu, lỗ hổng bảo mật thực hiện theo yêu cầu, hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.

Điều 17. Ứng phó, khắc phục sự cố an ninh mạng hệ thống thông tin quân sự

1. Hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quân sự, bao gồm:

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

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

c) Khoanh vùng, hạn chế phạm vi ảnh hưởng của sự cố;

d) Phân tích, đánh giá, phân loại sự cố an ninh mạng;

đ) Triển khai biện pháp ứng phó, khắc phục và khôi phục hệ thống;

e) Xác minh nguyên nhân, truy tìm nguồn gốc sự cố;

g) Điều tra, xử lý theo quy định của pháp luật trong trường hợp có dấu hiệu của tội phạm và hành vi vi phạm pháp luật.

2. Trình tự, thủ tục thực hiện ứng phó, khắc phục sự cố an ninh mạng

a) Phát hiện và tiếp nhận thông tin về sự cố an ninh mạng: Phát hiện thông qua hệ thống giám sát và tiếp nhận thông tin cảnh báo, báo cáo sự cố của chủ quản hệ thống thông tin quân sự;

b) Xác định và đánh giá nguy cơ: Phân tích dữ liệu, dấu hiệu bất thường để xác định sự cố và đánh giá phạm vi, mức độ ảnh hưởng của sự cố đối với hệ thống thông tin quân sự;

c) Tổ chức ứng cứu sự cố: Triển khai các biện pháp kỹ thuật để ngăn chặn, hạn chế sự lây lan của sự cố; cô lập thành phần hệ thống bị ảnh hưởng; loại bỏ mã độc, phần mềm độc hại hoặc hành vi xâm phạm trái phép;

d) Khắc phục và khôi phục hệ thống: Khắc phục các lỗ hổng, điểm yếu an ninh mạng; khôi phục dữ liệu, cấu hình hệ thống và dịch vụ bị ảnh hưởng; kiểm tra, đánh giá bảo đảm hệ thống hoạt động an toàn trước khi đưa vào vận hành trở lại;

đ) Báo cáo về sự cố an ninh mạng; phân tích nguyên nhân và đề xuất biện pháp phòng ngừa.

3. Chủ quản hệ thống thông tin quân sự có trách nhiệm thực hiện các hoạt động quy định tại khoản 1 Điều này. Trường hợp vượt quá khả năng, thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thực hiện ứng cứu sự cố an ninh mạng.

4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng có trách nhiệm tiếp nhận, xác minh thông tin về sự cố; hướng dẫn chủ quản hệ thống thông tin quân sự thực hiện biện pháp xử lý sự cố; tổ chức lực lượng, phương tiện, biện pháp kỹ thuật để triển khai ứng cứu sự cố.

Điều 18. Sử dụng mật mã để bảo vệ thông tin mạng

1. Dữ liệu, thông tin thuộc bí mật nhà nước phải được bảo vệ bằng mật mã cơ yếu khi lưu trữ, truyền đưa trên không gian mạng theo quy định của pháp luật về cơ yếu, bảo vệ bí mật nhà nước, dữ liệu.

2. Việc lưu trữ, truyền đưa dữ liệu, thông tin trong lĩnh vực quân sự, quốc phòng không thuộc bí mật nhà nước thực hiện theo quy định của Bộ Quốc phòng.

Điều 19. Thu thập dữ liệu điện tử trên không gian mạng thuộc phạm vi quản lý của Bộ Quốc phòng

1. Việc thu thập dữ liệu điện tử để phục vụ điều tra, xử lý các vụ việc vi phạm, tội phạm gây mất an toàn, an ninh, xâm phạm an ninh quốc gia, an ninh quân đội trên không gian mạng do lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thực hiện.

2. Trình tự, thủ tục thu thập dữ liệu điện tử để phục vụ điều tra, xử lý các vụ việc vi phạm, tội phạm gây mất an toàn, an ninh, xâm phạm an ninh quốc gia, an ninh quân đội trên không gian mạng được thực hiện theo quy định pháp luật.

3. Cục Bảo vệ an ninh Quân đội quyết định tiến hành biện pháp thu thập dữ liệu điện tử để phục vụ điều tra, xử lý các vụ việc vi phạm, tội phạm gây mất an toàn, an ninh, xâm phạm an ninh quốc gia, an ninh quân đội trên không gian mạng.

Điều 20. Biện pháp nghiệp vụ bảo vệ an ninh mạng

1. Bộ trưởng Bộ Quốc phòng quyết định áp dụng các biện pháp nghiệp vụ bảo vệ an ninh mạng để phục vụ bảo vệ an ninh mạng đối với hệ thống thông tin quân sự và điều tra, xác minh, xử lý các vụ việc trên không gian mạng thuộc phạm vi quản lý của Bộ Quốc phòng.

2. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng theo thẩm quyền chủ trì, tổ chức thực hiện nội dung các biện pháp nghiệp vụ bảo vệ an ninh mạng.

3. Trình tự, thủ tục áp dụng các biện pháp nghiệp vụ bảo vệ an ninh mạng

a) Phát hiện, tiếp nhận thông tin, cảnh báo hoặc xác định dấu hiệu nguy cơ, hành vi vi phạm pháp luật về an ninh mạng;

b) Tổ chức đánh giá nguy cơ, mức độ ảnh hưởng, phạm vi tác động;

c) Đề xuất biện pháp nghiệp vụ bảo vệ an ninh mạng phù hợp với tính chất, mức độ, nguy cơ hoặc hành vi vi phạm;

d) Xem xét, quyết định áp dụng biện pháp nghiệp vụ bảo vệ an ninh mạng theo thẩm quyền;

đ) Tổ chức triển khai biện pháp đã được quyết định;

e) Theo dõi, kiểm tra, đánh giá việc chấp hành thực hiện biện pháp;

g) Tổng hợp, báo cáo kết quả thực hiện nhiệm vụ theo quy định.

4. Thông tin, tài liệu, dữ liệu và kết quả thu được trong quá trình áp dụng các biện pháp nghiệp vụ bảo vệ an ninh mạng được quản lý, sử dụng theo quy định của pháp luật về bảo vệ bí mật nhà nước và quy định của Bộ Quốc phòng.

Mục 2
BẢO ĐẢM AN NINH DỮ LIỆU

Điều 21. Trách nhiệm bảo đảm an ninh dữ liệu

1. Chủ quản hệ thống thông tin, chủ quản dữ liệu và các tổ chức, cá nhân có liên quan có trách nhiệm bảo đảm an ninh dữ liệu thuộc phạm vi quản lý của Bộ Quốc phòng; phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng trong bảo đảm an ninh dữ liệu.

2. Đối với dữ liệu được xử lý trên không gian mạng thuộc phạm vi quản lý của Bộ Quốc phòng, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng hướng dẫn chủ quản hệ thống thông tin, chủ quản dữ liệu các tổ chức, cá nhân có liên quan áp dụng biện pháp kỹ thuật và biện pháp quản lý nhằm phòng ngừa, phát hiện và ngăn chặn các hành vi bị nghiêm cấm theo quy định của Luật An ninh mạng và pháp luật có liên quan.

Điều 22. Nội dung bảo đảm an ninh dữ liệu thuộc phạm vi quản lý của Bộ Quốc phòng

Bộ Quốc phòng chủ trì, tổ chức bảo đảm an ninh dữ liệu đối với hệ thống thông tin quân sự, các dữ liệu có ảnh hưởng đến nhiệm vụ quân sự, quốc phòng theo pháp luật về an ninh mạng, dữ liệu, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước, cơ yếu và các quy định sau:

1. Triển khai các biện pháp quản lý, kỹ thuật và nghiệp vụ để bảo đảm an ninh dữ liệu thuộc phạm vi quản lý của Bộ Quốc phòng; phân loại, quản lý và áp dụng biện pháp bảo vệ đối với dữ liệu quân sự, quốc phòng.

2. Quy định tiêu chuẩn, quy chuẩn kỹ thuật, yêu cầu bảo đảm an ninh dữ liệu phù hợp với hoạt động quân sự, quốc phòng.

3. Giám sát, kiểm tra, đánh giá rủi ro an ninh dữ liệu; phát hiện, phòng ngừa, ngăn chặn và xử lý các hành vi xâm phạm an ninh dữ liệu đối với hệ thống thông tin quân sự.

4. Bảo vệ, ứng cứu, khắc phục sự cố an ninh dữ liệu đối với hệ thống thông tin quân sự.

5. Quyết định việc sử dụng mật mã để bảo đảm an ninh thông tin, dữ liệu đối với hệ thống thông tin quân sự.

6. Thẩm định, kiểm tra, đánh giá, quyết định việc lưu trữ, xử lý, chia sẻ hoặc chuyển dữ liệu thuộc phạm vi quản lý ra bên ngoài.

7. Áp dụng các biện pháp bảo đảm an ninh nội bộ để phòng ngừa nguy cơ lộ, mất dữ liệu.

Mục 3
PHÒNG NGỪA, XỬ LÝ THÔNG TIN VÀ HÀNH VI SỬ DỤNG CÔNG NGHỆ THÔNG TIN, PHƯƠNG TIỆN ĐIỆN TỬ XÂM PHẠM AN NINH QUỐC GIA, TRẬT TỰ, AN TOÀN XÃ HỘI TRÊN KHÔNG GIAN MẠNG, BẢO ĐẢM AN NINH THÔNG TIN MẠNG

Điều 23. Thẩm quyền, trách nhiệm của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng

1. Chủ trì xử lý thông tin và đấu tranh phòng, chống hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội đối với hệ thống thông tin quân sự.

2. Chủ trì xử lý thông tin và đấu tranh phòng, chống hành vi trên không gian mạng trong trường hợp cơ quan có thẩm quyền xác định thông tin và hành vi sử dụng công nghệ thông tin, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội do tổ chức, cá nhân thuộc phạm vi quản lý của Bộ Quốc phòng thực hiện hoặc cản trở việc thực hiện nhiệm vụ, xâm phạm quyền, lợi ích hợp pháp của cơ quan, đơn vị, doanh nghiệp, tổ chức, cá nhân thuộc phạm vi quản lý của Bộ Quốc phòng.

3. Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong bảo vệ an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

4. Cục Bảo vệ an ninh Quân đội được áp dụng các biện pháp quy định tại khoản 1 Điều 5 Luật An ninh mạng để phục vụ phòng ngừa, điều tra, xử lý thông tin và 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 thuộc phạm vi quản lý của Bộ Quốc phòng.

5. Bộ Tư lệnh Tác chiến không gian mạng được áp dụng các biện pháp quy định tại khoản 1 Điều 5 Luật An ninh mạng phù hợp với hoạt động tác chiến không gian mạng.

6. Việc áp dụng đối với từng biện pháp tại khoản 1 Điều 5 Luật An ninh mạng của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thực hiện theo quy định của pháp luật và quy định của Bộ Quốc phòng.

Điều 24. Trách nhiệm của chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng

1. Chủ quản hệ thống thông tin, doanh nghiệp trong nước, doanh nghiệp nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, dịch vụ gia tăng trên không gian mạng có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng theo yêu cầu của cơ quan có thẩm quyền và theo quy định của pháp luật trong các vụ việc thuộc phạm vi quản lý của Bộ Quốc phòng.

2. Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet và dịch vụ gia tăng trên không gian mạng thuộc Bộ Quốc phòng có trách nhiệm định danh địa chỉ IP và thực hiện bảo đảm an ninh thông tin mạng theo quy định tại các khoản 2 và khoản 3 Điều 25 Luật An ninh mạng thông qua lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng để bảo vệ bí mật nhà nước, đảm bảo việc thực hiện nhiệm vụ quân sự, quốc phòng.

Điều 25. Trách nhiệm của tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng

1. Thực hiện yêu cầu gỡ bỏ, cải chính, chấm dứt phát tán thông tin có nội dung thuộc trường hợp theo quy định của pháp luật trong phạm vi quản lý của Bộ Quốc phòng và cung cấp thông tin, dữ liệu liên quan khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.

Thời hạn thực hiện nghĩa vụ gỡ bỏ không quá 06 giờ kể từ khi nhận được yêu cầu, trường hợp khẩn cấp thực hiện trong thời hạn không quá 01 giờ; đồng thời, có trách nhiệm thông báo kết quả thực hiện theo yêu cầu.

2. Chủ động thông báo, tố giác với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng khi phát hiện thông tin hoặc hành vi vi phạm pháp luật trên không gian mạng liên quan đến quân sự, quốc phòng.

3. Áp dụng các biện pháp kỹ thuật theo quy định của pháp luật để ngăn chặn việc tiếp tục lan truyền thông tin vi phạm trong phạm vi quản lý, bao gồm: Vô hiệu hóa chức năng chia sẻ, sao chép, phát tán; ngăn chặn việc đăng tải lại; loại bỏ liên kết, dữ liệu về nội dung vi phạm theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng.

4. Cung cấp thông tin, tài liệu, dữ liệu điện tử liên quan đến nội dung vi phạm bảo đảm toàn vẹn, đầy đủ, chính xác theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng trong thời hạn không quá 24 giờ, trường hợp khẩn cấp không quá 06 giờ.

Điều 26. Trách nhiệm của người quản trị, điều hành hội, nhóm, kênh, trang, tài khoản trên không gian mạng

1. Quản trị, điều hành hội, nhóm, kênh, trang, tài khoản trên không gian mạng theo pháp luật về an ninh mạng và pháp luật có liên quan.

2. Phối hợp, thực hiện theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng trong xử lý thông tin và hành vi thuộc trường hợp theo quy định của pháp luật trong phạm vi quản lý của Bộ Quốc phòng

a) Gỡ bỏ thông tin vi phạm; cung cấp thông tin, dữ liệu liên quan đến hội, nhóm, kênh, trang, tài khoản do mình quản lý;

b) Áp dụng các biện pháp kỹ thuật theo quy định của pháp luật để ngăn chặn việc lan truyền, đăng tải lại nội dung vi phạm.

3. Không xóa dấu vết, tiêu hủy dữ liệu hoặc cản trở hoạt động xác minh, điều tra.

Chương III
SẢN PHẨM, DỊCH VỤ AN NINH MẠNG VÀ KINH DOANH SẢN PHẨM, DỊCH VỤ AN NINH MẠNG PHỤC VỤ NHIỆM VỤ QUÂN SỰ

Điều 27. Sản phẩm, dịch vụ an ninh mạng phục vụ nhiệm vụ quân sự

1. Sản phẩm an ninh mạng, bao gồm:

a) Sản phẩm kiểm tra, đánh giá an ninh mạng gồm các thiết bị phần cứng, phần mềm có các chức năng cơ bản sau: Rà quét, kiểm tra, phân tích cấu hình, hiện trạng, dữ liệu nhật ký của hệ thống thông tin; phát hiện lỗ hổng, điểm yếu; đưa ra đánh giá rủi ro an ninh mạng;

b) Sản phẩm giám sát an ninh mạng gồm các thiết bị phần cứng, phần mềm có các chức năng cơ bản sau: Giám sát, phân tích dữ liệu lưu trữ, truyền trên hệ thống thông tin; thu thập, phân tích dữ liệu nhật ký theo thời gian thực; phát hiện và đưa ra cảnh báo sự kiện bất thường, có nguy cơ gây mất an ninh mạng;

c) Sản phẩm chống tấn công, xâm nhập gồm các thiết bị phần cứng, phần mềm có chức năng cơ bản ngăn chặn tấn công, xâm nhập vào hệ thống thông tin;

d) Các sản phẩm an ninh mạng khác theo quy định của Bộ Quốc phòng.

2. Dịch vụ an ninh mạng, bao gồm:

a) Dịch vụ kiểm tra, đánh giá an ninh mạng gồm dịch vụ rà quét, kiểm tra, phân tích cấu hình, hiện trạng, dữ liệu nhật ký của hệ thống thông tin; phát hiện lỗ hổng, điểm yếu; đưa ra đánh giá rủi ro mất an ninh mạng;

b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự gồm dịch vụ hỗ trợ người sử dụng bảo đảm tính bí mật của thông tin, hệ thống thông tin mà không sử dụng hệ thống mật mã dân sự;

c) Dịch vụ tư vấn an ninh mạng gồm dịch vụ hỗ trợ tư vấn, kiểm tra, đánh giá, triển khai, thiết kế, xây dựng các giải pháp bảo đảm an ninh mạng;

d) Dịch vụ giám sát an ninh mạng gồm dịch vụ giám sát, phân tích lưu lượng dữ liệu truyền trên hệ thống thông tin; thu thập, phân tích dữ liệu nhật ký theo thời gian thực; phát hiện và đưa ra cảnh báo sự kiện bất thường, có nguy cơ gây mất an ninh mạng;

đ) Dịch vụ ứng cứu sự cố an ninh mạng để xử lý, khắc phục sự cố gây mất an ninh mạng đối với hệ thống thông tin;

e) Dịch vụ khôi phục dữ liệu trong hệ thống thông tin đã bị xóa hoặc hư hỏng;

g) Dịch vụ phòng ngừa, chống tấn công mạng để ngăn chặn các hành vi tấn công, xâm nhập vào hệ thống thông tin thông qua việc giám sát, thu thập, phân tích các sự kiện đang xảy ra trên hệ thống thông tin;

h) Dịch vụ điều tra và phân tích số gồm dịch vụ thu thập, bảo quản, phân tích và phục hồi dữ liệu hoặc chứng cứ điện tử phục vụ xử lý sự cố an ninh mạng và các hoạt động khác theo quy định của pháp luật;

i) Dịch vụ đào tạo và diễn tập an ninh mạng gồm dịch vụ đào tạo, huấn luyện, nâng cao nhận thức; tổ chức diễn tập tình huống để tăng cường năng lực bảo đảm an ninh mạng;

k) Các dịch vụ an ninh mạng khác theo quy định của Bộ Quốc phòng.

Điều 28. Quản lý hoạt động kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng phục vụ nhiệm vụ quân sự

1. Doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng phải có giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng theo quy định của pháp luật về an ninh mạng. Sản phẩm, dịch vụ an ninh mạng cung cấp cho Bộ Quốc phòng phục vụ nhiệm vụ quân sự được miễn thực hiện thủ tục xin cấp phép của cơ quan quản lý nhà nước có thẩm quyền và không bắt buộc phải thể hiện thông tin trên Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng.

2. Bộ Quốc phòng thực hiện quản lý đối với sản phẩm, dịch vụ an ninh mạng quy định tại Điều này và có trách nhiệm sau:

a) Ban hành tiêu chuẩn, quy chuẩn kỹ thuật và quản lý chất lượng;

b) Đăng ký, chỉ định và quản lý hoạt động của các tổ chức chứng nhận hợp chuẩn, hợp quy;

c) Quản lý và cấp phép hoạt động xuất khẩu, nhập khẩu sản phẩm an ninh mạng;

d) Kiểm tra, giám sát hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng phục vụ nhiệm vụ quân sự.

Chương IV
NGĂN CHẶN XUNG ĐỘT THÔNG TIN TRÊN KHÔNG GIAN MẠNG

Mục 1
GIÁM SÁT, PHÁT HIỆN, CẢNH BÁO XUNG ĐỘT THÔNG TIN TRÊN KHÔNG GIAN MẠNG

Điều 29. Giám sát, phát hiện và cảnh báo xung đột thông tin trên không gian mạng

1. Hoạt động giám sát, phát hiện, cảnh báo xung đột thông tin trên không gian mạng là một nội dung của hoạt động giám sát an ninh mạng và phải được lực lượng chuyên trách bảo vệ an ninh mạng, chủ quản hệ thống thông tin thực hiện thường xuyên, liên tục theo quy định của pháp luật về an ninh mạng.

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, các cổng kết nối quốc tế có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng để xây dựng, triển khai, huấn luyện, duy trì hệ thống giám sát, phát hiện và cảnh báo xung đột thông tin trên không gian mạng.

3. Thông tin giám sát phải được lực lượng chuyên trách bảo vệ an ninh mạng tiếp nhận, phân tích, xử lý và cảnh báo đến các tổ chức, cá nhân liên quan.

Điều 30. Tiếp nhận và xử lý xung đột thông tin trên không gian mạng

1. Chủ quản hệ thống thông tin có trách nhiệm tiếp nhận, xử lý xung đột thông tin trên không gian mạng và phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng để ứng cứu sự cố và ngăn chặn xung đột thông tin trên không gian mạng.

2. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm tiếp nhận, phân tích, xử lý xung đột thông tin trên không gian mạng giữa các tổ chức, cá nhân trong nước và nước ngoài được quy định tại khoản 1 Điều 41 và khoản 1 Điều 42 Nghị định này.

3. Việc xử lý xung đột thông tin trên không gian mạng phải được lực lượng chuyên trách bảo vệ an ninh mạng thực hiện để không làm gia tăng mức độ xung đột và ngăn chặn không để xảy ra chiến tranh dưới mọi hình thức.

4. Bộ Quốc phòng chủ trì thiết lập đầu mối tiếp nhận, xử lý thông tin về xung đột thông tin trên không gian mạng thuộc phạm vi quản lý và liên quan đến chủ quyền quốc gia trên không gian mạng; phối hợp với Bộ Công an trong xử lý các vụ việc liên quan đến an ninh quốc gia, trật tự, an toàn xã hội.

5. Bộ Công an chủ trì xử lý xung đột thông tin trên không gian mạng liên quan đến an ninh quốc gia, trật tự, an toàn xã hội và phối hợp với Bộ Quốc phòng xử lý các vụ việc liên quan đến quốc phòng và chủ quyền quốc gia trên không gian mạng.

Mục 2
XÁC ĐỊNH NGUỒN GỐC THÔNG TIN TRÊN KHÔNG GIAN MẠNG

Điều 31. Nội dung xác định nguồn gốc xung đột thông tin trên không gian mạng

1. Nội dung xác định nguồn gốc xung đột thông tin trên không gian mạng bao gồm xác định gói tin, thông tin, địa chỉ nguồn, địa chỉ đích, cổng dịch vụ, thời gian và cách thức, thủ đoạn xung đột thông tin trên không gian mạng; xác định đối tượng, mục đích và mức độ gây xung đột thông tin trên không gian mạng.

2. Việc xác định nguồn gốc xung đột thông tin trên không gian mạng phải tuân thủ quy định của pháp luật về an ninh mạng, bảo vệ bí mật nhà nước và pháp luật có liên quan.

Điều 32. Kết quả xác định nguồn gốc xung đột thông tin trên không gian mạng

1. Kết quả xác định nguồn gốc xung đột thông tin trên không gian mạng là các tài liệu, bằng chứng, chứng cứ được các lực lượng chuyên trách bảo vệ an ninh mạng thu thập bảo đảm tính khách quan, chính xác và khoa học.

2. Kết quả xác định nguồn gốc xung đột thông tin trên không gian mạng được sử dụng hợp pháp trong đấu tranh, ngăn chặn xung đột thông tin trên không gian mạng.

Điều 33. Vai trò, trách nhiệm trong xác định nguồn gốc xung đột thông tin trên không gian mạng

1. Xác định nguồn gốc gây xung đột thông tin trên không gian mạng nhằm phát hiện, thu thập, đánh giá, sử dụng làm bằng chứng, chứng cứ.

2. Việc xác định nguồn gốc xung đột thông tin trên không gian mạng thuộc thẩm quyền của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Chủ quản hệ thống thông tin liên quan đến xung đột thông tin trên không gian mạng có trách nhiệm phối hợp với các lực lượng chuyên trách bảo vệ an ninh mạng để xác định chính xác nguồn gốc gây xung đột thông tin trên không gian mạng.

4. Cơ quan, tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm cung cấp kịp thời và đầy đủ cho lực lượng chuyên trách bảo vệ an ninh mạng về thông tin, bằng chứng, chứng cứ để phục vụ công tác xác định nguồn gốc.

5. Cơ quan, tổ chức, cá nhân tham gia hoặc có liên quan đến xung đột thông tin trên không gian mạng phải chịu trách nhiệm cung cấp thông tin chính xác, không được cung cấp thông tin sai lệch. Trường hợp cố ý cung cấp thông tin sai lệch tùy theo mức độ vi phạm bị truy cứu trách nhiệm hình sự hoặc xử lý hành chính.

Mục 3
CHẶN LỌC, KHẮC PHỤC VÀ LOẠI TRỪ XUNG ĐỘT THÔNG TIN TRÊN KHÔNG GIAN MẠNG

Điều 34. Chặn lọc thông tin trên không gian mạng

1. Chặn lọc thông tin được các doanh nghiệp cung cấp dịch vụ viễn thông, Internet thực hiện khi có một trong các yếu tố sau:

a) Xác định được nguồn gốc xung đột thông tin trên không gian mạng gây ảnh hưởng đến quốc phòng, an ninh và chủ quyền quốc gia trên không gian mạng;

b) Khi xác định rõ tính hợp lý về yêu cầu của bên bị xung đột thông tin trên không gian mạng;

c) Có yêu cầu bằng văn bản hoặc yêu cầu thông qua hệ thống kỹ thuật phục vụ chỉ huy, điều hành của lực lượng chuyên trách bảo vệ an ninh mạng.

2. Việc chặn lọc thông tin phải bảo đảm đúng thẩm quyền, đúng đối tượng, không làm ảnh hưởng đến hoạt động hợp pháp của tổ chức, cá nhân.

Điều 35. Khắc phục xung đột thông tin trên không gian mạng

1. Chủ quản hệ thống thông tin chịu trách nhiệm trong việc tổ chức khắc phục xung đột thông tin trên không gian mạng thuộc phạm vi quản lý và chịu sự điều hành của lực lượng chuyên trách bảo vệ an ninh mạng trong việc tổ chức khắc phục xung đột thông tin trên không gian mạng.

2. Chủ quản hệ thống thông tin chịu trách nhiệm xây dựng các phương án khắc phục xung đột thông tin trên không gian mạng thuộc phạm vi quản lý và có trách nhiệm tổng hợp, báo cáo tình hình, kết quả khắc phục xung đột thông tin trên không gian mạng cho lực lượng chuyên trách bảo vệ an ninh mạng.

3. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm phối hợp với cơ quan chủ quản hệ thống thông tin khắc phục xung đột thông tin liên quan tới quốc phòng, an ninh quốc gia và cơ quan nhà nước theo quy định tại khoản 1 Điều 41 và khoản 1 Điều 42 Nghị định này.

4. Biện pháp khắc phục xung đột thông tin được áp dụng khi có đủ các điều kiện sau đây:

a) Xác định có xung đột thông tin xảy ra;

b) Xung đột thông tin gây ảnh hưởng hoặc có nguy cơ ảnh hưởng đến hoạt động của cơ quan, tổ chức, cá nhân;

c) Có yêu cầu hoặc chỉ đạo của cơ quan có thẩm quyền đối với vụ việc liên quan đến quốc phòng, an ninh.

Điều 36. Loại trừ xung đột thông tin trên không gian mạng

1. Các lực lượng chuyên trách bảo vệ an ninh mạng chịu trách nhiệm loại trừ xung đột thông tin trên không gian mạng.

2. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet có trách nhiệm phối hợp với các lực lượng chuyên trách bảo vệ an ninh mạng để loại trừ.

3. Loại trừ xung đột thông tin trên không gian mạng được thực hiện khi có các yếu tố sau:

a) Xác định rõ nguồn gốc xung đột thông tin trên không gian mạng;

b) Nhân lực, biện pháp công nghệ, kỹ thuật và đấu tranh ngoại giao có đủ khả năng để loại trừ xung đột thông tin trên không gian mạng;

c) Thông báo trực tiếp hoặc gián tiếp qua điện thoại, email hoặc hệ thống thông tin đại chúng đến tổ chức, cá nhân có liên quan đối với nguồn thông tin gây xung đột thông tin trên không gian mạng.

Điều 37. Công tác phối hợp trong chặn lọc, khắc phục và loại trừ xung đột thông tin trên không gian mạng

1. Bộ Quốc phòng chủ trì chặn lọc, khắc phục và loại trừ xung đột thông tin trên không gian mạng có liên quan đến cơ quan, đơn vị, doanh nghiệp, cá nhân, chức năng, nhiệm vụ của Bộ Quốc phòng; phối hợp với Bộ Công an trong các vụ việc có liên quan đến an ninh quốc gia, trật tự, an toàn xã hội.

2. Bộ Công an chủ trì chặn lọc, khắc phục và loại trừ xung đột thông tin trên không gian mạng liên quan đến an ninh quốc gia, trật tự, an toàn xã hội; phối hợp với Bộ Quốc phòng trong các vụ việc có liên quan đến quốc phòng.

3. Bộ Khoa học và Công nghệ có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, Bộ Quốc phòng theo quy định tại khoản 1, 2 Điều này trong hướng dẫn, điều phối kỹ thuật và yêu cầu doanh nghiệp cung cấp dịch vụ viễn thông, Internet thực hiện các biện pháp chặn lọc, khắc phục, loại trừ theo yêu cầu của cơ quan có thẩm quyền.

4. Bộ Văn hóa, Thể thao và Du lịch có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, Bộ Quốc phòng theo quy định tại khoản 1, 2 Điều này trong quản lý, chặn lọc, khắc phục và loại trừ thông tin xung đột trên báo chí, phát thanh, truyền hình và môi trường thông tin điện tử theo quy định của pháp luật.

5. Chủ quản hệ thống thông tin có trách nhiệm phối hợp thực hiện các biện pháp chặn lọc, khắc phục và loại trừ xung đột thông tin trong phạm vi quản lý theo yêu cầu của cơ quan có thẩm quyền.

6. Doanh nghiệp cung cấp dịch vụ viễn thông, Internet có trách nhiệm thực hiện các biện pháp kỹ thuật, cung cấp thông tin, dữ liệu và phối hợp với cơ quan có thẩm quyền trong quá trình chặn lọc, khắc phục và loại trừ xung đột thông tin.

Mục 4
THÔNG TIN, TUYÊN TRUYỀN, GIÁO DỤC, ĐỊNH HƯỚNG DƯ LUẬN VÀ HỢP TÁC QUỐC TẾ VỀ NGĂN CHẶN XUNG ĐỘT THÔNG TIN TRÊN KHÔNG GIAN MẠNG

Điều 38. Thông tin, tuyên truyền, giáo dục và định hướng dư luận về ngăn chặn xung đột thông tin trên không gian mạng

1. Nội dung thông tin, tuyên truyền, giáo dục và định hướng dư luận

a) Chính sách, pháp luật về ngăn chặn xung đột thông tin trên không gian mạng;

b) Vị trí, vai trò, tầm quan trọng của công tác ngăn chặn xung đột thông tin trên không gian mạng;

c) Phương thức, thủ đoạn và nguy cơ gây xung đột thông tin trên không gian mạng;

d) Kiến thức, kỹ năng chủ động ngăn chặn xung đột thông tin trên không gian mạng;

đ) Biện pháp, kinh nghiệm ngăn chặn xung đột thông tin trên không gian mạng;

e) Trách nhiệm của cơ quan, tổ chức, doanh nghiệp và cá nhân trong ngăn chặn xung đột thông tin trên không gian mạng;

g) Các nội dung khác có liên quan đến ngăn chặn xung đột thông tin trên không gian mạng.

2. Hình thức thông tin, tuyên truyền, giáo dục và định hướng dư luận

a) Gặp gỡ, trao đổi, đối thoại, thảo luận trực tiếp;

b) Thông qua các phương tiện thông tin đại chúng;

c) Thông qua hoạt động tại các cơ sở giáo dục, đào tạo, hiệp hội an ninh mạng;

d) Thông qua các cuộc thi tìm hiểu pháp luật, sinh hoạt cộng đồng;

đ) Các hình thức khác phù hợp với quy định của pháp luật.

3. Tăng cường công tác thông tin, tuyên truyền, giáo dục và định hướng dư luận đối với các chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ viễn thông, Internet; các hiệp hội, câu lạc bộ trong lĩnh vực công nghệ thông tin, an ninh mạng, điện tử viễn thông và những địa bàn thường xảy ra nhiều vụ việc gây xung đột thông tin trên không gian mạng.

4. Bộ Quốc phòng, Bộ Công an có trách nhiệm phối hợp với Bộ Giáo dục và Đào tạo, các ban, bộ, ngành liên quan tổ chức thông tin, tuyên truyền, giáo dục và định hướng dư luận về ngăn chặn xung đột thông tin trên không gian mạng theo quyền hạn, trách nhiệm được quy định tại khoản 1 Điều 41 và khoản 1 Điều 42 Nghị định này nhằm nâng cao nhận thức, trách nhiệm và hiệu quả ngăn chặn xung đột thông tin trên không gian mạng.

Điều 39. Nội dung hợp tác quốc tế về ngăn chặn xung đột thông tin trên không gian mạng

1. Hợp tác quốc tế thu thập, nghiên cứu, trao đổi thông tin, kinh nghiệm về ngăn chặn xung đột thông tin trên không gian mạng; phối hợp đào tạo, bồi dưỡng, huấn luyện nghiệp vụ về ngăn chặn xung đột thông tin trên không gian mạng; tổ chức hội nghị, hội thảo quốc tế về các vấn đề liên quan đến ngăn chặn xung đột thông tin trên không gian mạng; hỗ trợ về cơ sở vật chất, kỹ thuật, công nghệ nhằm tăng cường lực lượng cho lực lượng chuyên trách bảo vệ an ninh mạng.

2. Hợp tác quốc tế nhằm loại trừ nguy cơ xung đột thông tin mạng trên lãnh thổ của một nước nhằm vào nước khác; phối hợp điều tra khi có yêu cầu ngăn chặn xung đột thông tin mạng từ quốc tế, phải tuân thủ quy định của pháp luật về an ninh mạng, pháp luật về quốc phòng và điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

3. Tham vấn về các hoạt động ngăn chặn xung đột thông tin trên không gian mạng và hợp tác giải quyết những vấn đề liên quan đến ngăn chặn xung đột thông tin trên không gian mạng với các quốc gia.

Điều 40. Từ chối hợp tác quốc tế về ngăn chặn xung đột thông tin trên không gian mạng

Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan, tổ chức có liên quan của Việt Nam có quyền từ chối hợp tác đối với các yêu cầu hợp tác có nội dung gây phương hại đến chủ quyền, quốc phòng, an ninh quốc gia, lợi ích của Nhà nước hoặc có nội dung không phù hợp với quy định của pháp luật Việt Nam và điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

Mục 5
TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN VÀ DOANH NGHIỆP CUNG CẤP DỊCH VỤ VIỄN THÔNG, INTERNET TRONG NGĂN CHẶN XUNG ĐỘT THÔNG TIN TRÊN KHÔNG GIAN MẠNG

Điều 41. Bộ Quốc phòng

1. Bộ Quốc phòng chịu trách nhiệm trước Chính phủ chủ trì, phối hợp với các cơ quan liên quan ngăn chặn xung đột thông tin trên không gian mạng với các mục đích sau đây:

a) Phòng, chống chiến tranh thông tin, chiến tranh không gian mạng;

b) Ngăn chặn các lực lượng quân sự nước ngoài hoặc các tổ chức trong nước, nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin quân sự.

2. Chủ trì ngăn chặn xung đột thông tin trên không gian mạng để bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ của Bộ Quốc phòng.

3. Tổ chức xây dựng lực lượng nghiệp vụ có tính chiến đấu cao, điều phối và sử dụng các nguồn lực quốc phòng để ngăn chặn xung đột thông tin trên không gian mạng với các mục đích quy định tại khoản 1 Điều này.

4. Xây dựng, sửa đổi, bổ sung, trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền văn bản về hoạt động ngăn chặn xung đột thông tin trên không gian mạng.

5. Chủ trì, phối hợp với các cơ quan liên quan tổ chức đào tạo, bồi dưỡng nguồn nhân lực thực hiện nhiệm vụ ngăn chặn xung đột thông tin trên không gian mạng.

6. Chỉ đạo lực lượng thuộc quyền chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tổ chức huấn luyện, diễn tập nghiệp vụ ngăn chặn xung đột thông tin trên không gian mạng.

7. Đầu tư, trang bị phương tiện cho thực hiện nhiệm vụ ngăn chặn xung đột thông tin trên không gian mạng.

8. Trao đổi thông tin với Bộ Công an, Bộ Ngoại giao và các ban, bộ, ngành liên quan trong ngăn chặn xung đột thông tin trên không gian mạng.

9. Thực hiện hợp tác quốc tế về ngăn chặn xung đột thông tin trên không gian mạng.

Điều 42. Bộ Công an

1. Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp với các cơ quan liên quan ngăn chặn xung đột thông tin trên không gian mạng giữa hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến an ninh quốc gia, trật tự, an toàn xã hội theo chức năng, nhiệm vụ của Bộ Công an.

2. Chủ trì ngăn chặn xung đột thông tin trên không gian mạng nhằm bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm.

3. Chủ trì, phối hợp với Bộ Quốc phòng, các cơ quan, tổ chức liên quan xây dựng và tổ chức thực hiện các biện pháp nhằm phát hiện, ngăn chặn, đấu tranh, loại trừ các hoạt động trên không gian mạng đe dọa đến an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm; xử lý các hành vi xâm phạm chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao theo quy định của pháp luật về an ninh mạng và phù hợp với phạm vi quản lý.

4. Chỉ đạo các lực lượng thuộc quyền chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng tổ chức huấn luyện, diễn tập nghiệp vụ ngăn chặn xung đột thông tin trên không gian mạng và bảo vệ an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm; thực hiện hợp tác quốc tế về ngăn chặn xung đột thông tin trên không gian mạng.

5. Thường xuyên trao đổi, cung cấp thông tin với Bộ Quốc phòng về tình hình, nguy cơ mất an ninh thông tin và các hoạt động có liên quan đến ngăn chặn xung đột thông tin trên không gian mạng.

Điều 43. Bộ Ngoại giao

Chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an tổ chức triển khai giải pháp bảo vệ cho hệ thống thông tin trong các cơ quan đại diện nước Cộng hòa xã hội chủ nghĩa Việt Nam ở nước ngoài; phối hợp thực hiện công tác đối ngoại liên quan đến hoạt động ngăn chặn xung đột thông tin trên không gian mạng.

Điều 44. Bộ Khoa học và Công nghệ

1. Tham mưu cho Chính phủ xác định các nhiệm vụ khoa học và công nghệ liên quan đến hoạt động ngăn chặn xung đột thông tin trên không gian mạng.

2. Chỉ đạo các cơ quan, đơn vị thuộc quyền quản lý phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng, Bộ Công an thực hiện các nhiệm vụ khoa học và công nghệ, xây dựng tiềm lực khoa học và công nghệ trong việc bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 45. Bộ Tài chính

Trên cơ sở đề nghị của các bộ, cơ quan trung ương, Bộ Tài chính chủ trì trình cấp có thẩm quyền bố trí kinh phí trong dự toán ngân sách nhà nước hằng năm của các ban, bộ, cơ quan trung ương cho các hoạt động ngăn chặn xung đột thông tin trên không gian mạng theo quy định của pháp luật về ngân sách nhà nước.

Điều 46. Các ban, bộ, ngành và Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương

1. Giao nhiệm vụ cho cơ quan tham mưu quản lý nhà nước về công nghệ thông tin, an ninh mạng thực hiện ngăn chặn xung đột thông tin trên không gian mạng, bao gồm: Giám sát, phát hiện, cảnh báo, xác định nguồn gốc và khắc phục xung đột thông tin trên không gian mạng.

2. Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tổ chức triển khai các phương án bảo vệ các hệ thống thông tin trong phạm vi quản lý; sẵn sàng huy động lực lượng, phương tiện tham gia hoạt động ngăn chặn xung đột thông tin trên không gian mạng theo quy định của pháp luật.

3. Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng triển khai và đôn đốc thực hiện chính sách, chiến lược, kế hoạch ngăn chặn xung đột thông tin trên không gian mạng; xử lý, khắc phục các vụ việc liên quan đến xung đột thông tin trên không gian mạng trong phạm vi quản lý.

Điều 47. Tổ chức, cá nhân

1. Chủ quản hệ thống thông tin phải thực hiện các biện pháp bảo vệ hệ thống thông tin và ngăn chặn xung đột thông tin trên không gian mạng thuộc quyền quản lý; phối hợp chặt chẽ với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, Bộ Quốc phòng để triển khai các biện pháp ngăn chặn xung đột thông tin trên không gian mạng.

2. Cơ quan, tổ chức, cá nhân phải có trách nhiệm ngăn chặn các hành động gây nguy cơ xung đột thông tin trên không gian mạng có nguồn gốc từ hệ thống thông tin của mình, cũng như hợp tác xác định nguồn gốc xung đột thông tin trên không gian mạng, khắc phục hậu quả xung đột thông tin trên không gian mạng.

Điều 48. Doanh nghiệp cung cấp dịch vụ viễn thông, Internet

1. Cung cấp đầy đủ thông tin, phối hợp xác định và ngăn chặn các nguồn thông tin gây xung đột trên không gian mạng theo yêu cầu của các lực lượng chuyên trách bảo vệ an ninh mạng.

2. Triển khai các giải pháp bảo đảm an ninh mạng; tổ chức giám sát, phát hiện và kịp thời thông báo đến các lực lượng chuyên trách bảo vệ an ninh mạng về các nguồn thông tin gây xung đột trên không gian mạng.

3. Phối hợp với Bộ Quốc phòng, Bộ Công an triển khai các giải pháp, biện pháp công nghệ, kỹ thuật thông tin để ngăn chặn xung đột thông tin trên không gian mạng.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 49. Hiệu lực thi hành và điều khoản chuyển tiếp

1. Nghị định này có hiệu lực thi hành từ ngày 03 tháng 9 năm 2026. Nghị định số 142/2016/NĐ-CP ngày 01 tháng 12 năm 2016 của Chính phủ quy định về ngăn chặn xung đột thông tin trên mạng hết hiệu lực kể từ khi Nghị định này có hiệu lực.

2. Hệ thống thông tin quân sự đã được xác định cấp độ thì giữ cấp độ đã được xác định kể từ ngày Nghị định này có hiệu lực thi hành; trong thời hạn 12 tháng kể từ ngày Nghị định này có hiệu lực thi hành thì phải bảo đảm điều kiện, tiêu chuẩn, biện pháp bảo vệ an ninh mạng tương ứng với cấp độ theo quy định của Bộ Quốc phòng.

Điều 50. Tổ chức thực hiện

1. Bộ trưởng Bộ Quốc phòng chịu trách nhiệm đôn đốc, kiểm tra, hướng dẫn việc thực hiện Nghị định này.

2. Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương chịu trách nhiệm thi hành Nghị định này.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các tổ chức chính trị - xã hội;
- VPCP: BTCN, các PCN, Trợ lý TTg, các Vụ, Cục, Công báo;
- Lưu: VT, CĐS (2b).AH

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Phan Văn Giang