**LUẬT AN NINH MẠNG**

**DỰ THẢO 1**

**Ngày 06.6.2017**

[Chương I 2](#__RefHeading__3690_313856880)

[NHỮNG QUY ĐỊNH CHUNG 2](#__RefHeading__3692_313856880)

[Điều 1. Phạm vi điều chỉnh 2](#__RefHeading__3694_313856880)

[Điều 2. Đối tượng áp dụng 2](#__RefHeading__3696_313856880)

[Điều 3. Giải thích từ ngữ 2](#__RefHeading__3698_313856880)

[Điều 4. Chính sách an ninh mạng 4](#__RefHeading__3700_313856880)

[Điều 5. Nguyên tắc bảo vệ an ninh mạng 5](#__RefHeading__3702_313856880)

[Điều 6. Biện pháp bảo vệ an ninh mạng 5](#__RefHeading__3704_313856880)

[Điều 7. Các hành vi bị nghiêm cấm 5](#__RefHeading__3706_313856880)

[Điều 8. Xử lý vi phạm pháp luật về an ninh mạng 5](#__RefHeading__3708_313856880)

[Chương II 5](#__RefHeading__3710_313856880)

[BẢO VỆ AN NINH MẠNG 5](#__RefHeading__3712_313856880)

[Mục 1 6](#__RefHeading__3714_313856880)

[PHÒNG NGỪA, ĐẤU TRANH VỚI HOẠT ĐỘNG 6](#__RefHeading__3716_313856880)

[SỬ DỤNG KHÔNG GIAN MẠNG XÂM PHẠM AN NINH QUỐC GIA 6](#__RefHeading__3718_313856880)

[Điều 9. Xử lý thông tin kích động tụ tập đông người gây rối an ninh, trật tự trên không gian mạng 6](#__RefHeading__3720_313856880)

[Điều 10. Xử lý thông tin 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 6](#__RefHeading__3722_313856880)

[Điều 11. Phòng, chống gián điệp mạng, bảo vệ thông tin, tài liệu thuộc bí mật nhà nước trên không gian mạng 7](#__RefHeading__3724_313856880)

[Điều 12. Phòng, chống tấn công mạng 8](#__RefHeading__3726_313856880)

[Điều 13. Phòng, chống khủng bố mạng 9](#__RefHeading__3728_313856880)

[Điều 14. Phòng, chống chiến tranh mạng 9](#__RefHeading__3730_313856880)

[Điều 15. Tình huống khẩn cấp về an ninh mạng 9](#__RefHeading__3732_313856880)

[Điều 16. Các biện pháp áp dụng khi gia tăng nguy cơ xảy ra tình huống khẩn cấp về an ninh mạng 10](#__RefHeading__3734_313856880)

[Điều 17. Bảo đảm nguồn lực bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng 10](#__RefHeading__3736_313856880)

[Mục 2 10](#__RefHeading__3738_313856880)

[BẢO VỆ HỆ THỐNG THÔNG TIN QUAN TRỌNG 10](#__RefHeading__3740_313856880)

[VỀ AN NINH QUỐC GIA 10](#__RefHeading__3742_313856880)

[Điều 18. Hệ thống thông tin quan trọng về an ninh quốc gia 11](#__RefHeading__3744_313856880)

[Điều 19. Nguyên tắc bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia 11](#__RefHeading__3746_313856880)

[Điều 20. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 11](#__RefHeading__3748_313856880)

[Điều 21. Kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 12](#__RefHeading__3750_313856880)

[Điều 22. Giám sát, cảnh báo, ứng cứu, khắc phục sự cố xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia 12](#__RefHeading__3752_313856880)

[Mục 3 13](#__RefHeading__3754_313856880)

[GIÁM SÁT, DỰ BÁO, ỨNG CỨU 13](#__RefHeading__3756_313856880)

[VÀ DIỄN TẬP ỨNG CỨU SỰ CỐ AN NINH MẠNG 13](#__RefHeading__3758_313856880)

[Điều 23. Giám sát an ninh mạng 13](#__RefHeading__3760_313856880)

[Điều 24. Dự báo an ninh mạng 13](#__RefHeading__3762_313856880)

[Điều 25. Ứng cứu, khắc phục sự cố an ninh mạng 14](#__RefHeading__3764_313856880)

[Điều 26. Diễn tập ứng cứu sự cố an ninh mạng 14](#__RefHeading__3766_313856880)

[Điều 27. Ngừng cung cấp thông tin mạng 14](#__RefHeading__3768_313856880)

[Mục 4 14](#__RefHeading__3770_313856880)

[TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN NINH MẠNG 14](#__RefHeading__3772_313856880)

[VÀ CẤP PHÉP KINH DOANH DỊCH VỤ BẢO ĐẢM AN NINH MẠNG 15](#__RefHeading__3774_313856880)

[Điều 28. Xây dựng tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng 15](#__RefHeading__3776_313856880)

[Điều 29. Chứng nhận, công bố hợp chuẩn, hợp quy về an ninh mạng 15](#__RefHeading__3778_313856880)

[Điều 30. Đánh giá hợp chuẩn, hợp quy về an ninh mạng 15](#__RefHeading__3780_313856880)

[Điều 31. Yêu cầu bảo đảm an ninh mạng trong sản xuất, kinh doanh sản phẩm, dịch vụ mạng 16](#__RefHeading__3782_313856880)

[Điều 32. Dịch vụ bảo đảm an ninh mạng 16](#__RefHeading__3784_313856880)

[Điều 33. Điều kiện cấp giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng 17](#__RefHeading__3786_313856880)

[Điều 34. Hồ sơ đề nghị cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng 17](#__RefHeading__3788_313856880)

[Điều 35. Thẩm định hồ sơ và cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng 18](#__RefHeading__3790_313856880)

[Điều 36. Sửa đổi, bổ sung, gia hạn, tạm đình chỉ, thu hồi và cấp lại Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng 18](#__RefHeading__3792_313856880)

[Chương III 19](#__RefHeading__3794_313856880)

[TRIỂN KHAI CÔNG TÁC AN NINH MẠNG 19](#__RefHeading__3796_313856880)

[Điều 37. Triển khai công tác an ninh mạng trong hệ thống cơ quan nhà nước 19](#__RefHeading__3798_313856880)

[Điều 38. Nghiên cứu chiến lược phát triển và bảo vệ an ninh mạng 19](#__RefHeading__3800_313856880)

[Điều 39. An ninh thông tin mạng 21](#__RefHeading__3802_313856880)

[Điều 40. Giáo dục và nâng cao nhận thức về an ninh mạng 21](#__RefHeading__3804_313856880)

[Điều 41. Bảo đảm an ninh mạng trong ứng dụng, quản lý, vận hành điện toán đám mây 22](#__RefHeading__3806_313856880)

[Điều 42. Bảo đảm an ninh mạng đối với hệ thống liên kết thế giới thực và ảo 22](#__RefHeading__3808_313856880)

[Điều 43. Bảo đảm an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng internet quốc tế 22](#__RefHeading__3810_313856880)

[Điều 44. Nghiên cứu và phát triển quản lý định danh 22](#__RefHeading__3812_313856880)

[Điều 45. Bảo vệ an ninh mạng theo cấp độ 23](#__RefHeading__3814_313856880)

[Điều 46. Kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin thuộc cơ quan, tổ chức, doanh nghiệp nhà nước 23](#__RefHeading__3816_313856880)

[Điều 47. Nâng cao năng lực tự chủ về an ninh mạng 25](#__RefHeading__3818_313856880)

[Điều 48. Hợp tác quốc tế về an ninh mạng 25](#__RefHeading__3820_313856880)

[Chương IV 26](#__RefHeading__3822_313856880)

[ĐÀO TẠO, PHÁT TRIỂN NGUỒN NHÂN LỰC AN NINH MẠNG 26](#__RefHeading__3824_313856880)

[Điều 49. Chính sách đào tạo, phát triển nguồn nhân lực an ninh mạng 26](#__RefHeading__3826_313856880)

[Điều 50. Phát triển nguồn nhân lực an ninh mạng 26](#__RefHeading__3828_313856880)

[Điều 51. Văn bằng, chứng chỉ về an ninh mạng 26](#__RefHeading__3830_313856880)

[Điều 52. Phổ biến kiến thức an ninh mạng 26](#__RefHeading__3832_313856880)

[Chương V 27](#__RefHeading__3834_313856880)

[TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN 27](#__RefHeading__3836_313856880)

[Điều 53. Quyền và trách nhiệm của tổ chức, cá nhân tham gia sử dụng không gian mạng 27](#__RefHeading__3838_313856880)

[Điều 54. Trách nhiệm của chủ thể sản xuất, kinh doanh sản phẩm, dịch vụ mạng 27](#__RefHeading__3840_313856880)

[Điều 55. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, internet 28](#__RefHeading__3842_313856880)

[Điều 56. Trách nhiệm của cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia 28](#__RefHeading__3844_313856880)

[Điều 57. Trách nhiệm của Bộ Công an 29](#__RefHeading__3846_313856880)

[Điều 58. Trách nhiệm của Bộ Quốc phòng 30](#__RefHeading__3848_313856880)

[Điều 59. Trách nhiệm của Bộ Thông tin và Truyền thông 30](#__RefHeading__3850_313856880)

[Điều 60. Trách nhiệm của các bộ, ngành liên quan 31](#__RefHeading__3852_313856880)

[Điều 61. Trách nhiệm của ủy ban nhân dân cấp tỉnh 32](#__RefHeading__3854_313856880)

[Điều 62. Trách nhiệm của cơ quan chuyên trách bảo vệ an ninh mạng 32](#__RefHeading__3856_313856880)

[Chương VI 32](#__RefHeading__3858_313856880)

[ĐIỀU KHOẢN THI HÀNH 32](#__RefHeading__3860_313856880)

[Điều 63. Hiệu lực thi hành 33](#__RefHeading__3862_313856880)

[Điều 64. Quy định chi tiết 33](#__RefHeading__3864_313856880)

|  |  |
| --- | --- |
| **QUỐC HỘI** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** |
|  | **Độc lập - Tự do - Hạnh phúc** |
| Số: /2018/QH14 |  |

**LUẬT**

**AN NINH MẠNG**

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

*Quốc hội ban hành Luật An ninh mạng.*

# *Chương I*

# NHỮNG QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh

Luật này quy định về nguyên tắc, biện pháp, nội dung công tác an ninh mạng, hoạt động bảo đảm triển khai công tác an ninh mạng và trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan tới hoạt động quản lý, cung cấp, sử dụng không gian mạng và bảo vệ an ninh mạng của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

### Điều 2. Đối tượng áp dụng

Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan tới hoạt động quản lý, cung cấp, sử dụng không gian mạng và bảo vệ an ninh mạng của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

### Điều 3. Giải thích từ ngữ

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

1. *Không gian mạng* là mạng lưới kết nối toàn cầu của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng internet, mạng viễn thông, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, là môi trường đặc biệt mà con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

2. *Không gian mạng quốc gia* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng internet, mạng viễn thông, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, được xác định bằng phạm vi không gian mạng do Nhà nước quản lý, kiểm soát bằng chính sách, pháp luật và năng lực công nghệ.

3. *An ninh mạng* là khả năng bảo đảm hệ thống thông tin, thông tin và hoạt động trên không gian mạng không gây phương hại đến chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

4. *An ninh mạng quốc gia* là một bộ phận không thể tách rời của an ninh quốc gia; bao gồm sự bất khả xâm phạm về chủ quyền quốc gia trên không gian mạng, bảo đảm mọi thông tin và hoạt động trên không gian mạng không gây phương hại đến sự ổn định, phát triển bền vững của chế độ xã hội chủ nghĩa và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc, trật tự, an toàn xã hội.

5. *Bảo vệ an ninh mạng* là phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại âm mưu, hoạt động sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

6. *Thông tin trên không gian mạng* là thông tin được lưu trữ, truyền đưa, thu thập và xử lý thông qua không gian mạng.

7. *An ninh thông tin mạng* là sự bảo đảm thông tin trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

8*. Cơ sở hạ tầng không gian mạng quốc gia* là hệ thống trang thiết bị phục vụ cho việc tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin, 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 doanh nghiệp cung cấp dịch vụ viễn thông, 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 doanh nghiệp cung cấp dịch vụ viễn thông, internet;

c) Các dịch vụ, hệ thống ứng dụng công nghệ thông tin: dịch vụ trực tuyến (chính phủ điện tử, thương mại điện tử, báo điện tử, diễn đàn trực tuyến, mạng xã hội, blog…), hệ thống ứng dụng công nghệ thông tin có kết nối mạng phục vụ điều hành, quản lý, khai thác, vận hành của các cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng (bao gồm cả hệ thống điều khiển và giám sát tự động SCADA); cơ sở dữ liệu quốc gia.

9. *Hệ thống thông tin quan trọng về an ninh quốc gia* là hệ thống thông tin khi bị phá hoại sẽ làm ảnh hưởng đến chủ quyền, lợi ích, an ninh quốc gia và tác động nghiêm trọng tới trật tự, an toàn xã hội.

10. *Cổng kết nối mạng quốc tế* là nơi diễn ra hoạt động chuyển nhận tín hiệu mạng qua lại giữa Việt Nam và quốc gia khác.

11. *Tội phạm mạng* là hành vi sử dụng không gian mạng và công nghệ thông tin để thực hiện các hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự.

12. *Tấn công mạng* là hoạt động tấn công có chủ đích thông qua mạng nhằm phá vỡ tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin và hệ thống thông tin.

13. *Khủng bố mạng* là hoạt động sử dụng không gian mạng để thực hiện hành vi khủng bố, tài trợ khủng bố.

14. *Gián điệp mạng* là bất kỳ hành vi nào nhằm bí mật thu thập hoặc tìm cách thu thập thông tin trên không gian mạng vì lợi ích của thực thể nhà nước hoặc phi nhà nước.

15*. Chiến tranh mạng* là trạng thái xã hội đặc biệt của đất nước khi lực lượng quân sự nước ngoài sử dụng không gian mạng cùng với hoạt động vũ trang nhằm gây chiến tranh xâm lược.

16. *Tác chiến trên không gian mạng* là hoạt động chủ động đấu tranh có tổ chức trên không gian mạng nằm trong thế trận an ninh nhân dân và nền quốc phòng toàn dân nhằm bảo vệ lợi ích, chủ quyền và an ninh quốc gia.

17. *Tài khoản số* là thông tin dùng để chứng thực, phân quyền sử dụng các ứng dụng, dịch vụ bao gồm:

a) Tài khoản đăng nhập các trang web, blog, mạng xã hội;

b) Tài khoản tài chính (tài khoản ngân hàng trực tuyến, tài khoản tiền ảo, tài khoản giao dịch tài chính trên mạng);

c) Tài khoản đăng nhập các hệ điều hành máy tính, thiết bị di động thông minh như điện thoại, máy tính bảng, đồng hồ thông minh;

d) Tài khoản thư điện tử, dịch vụ điện tử;

đ) Tài khoản trò chơi trực tuyến trên mạng;

e) Các tài khoản trực tuyến khác.

18. *Sản phẩm, dịch vụ mạng* là phần cứng, thiết bị, phần mềm phục vụ hoạt động của không gian mạng hoặc được lưu trữ, truyền đưa trên không gian mạng.

19. *Nguy cơ đe dọa an ninh mạng* là các mối đe dọa đối với chủ quyền, lợi ích, an ninh quốc gia, thông tin và hệ thống thông tin hoặc bất kỳ hậu quả nào xảy ra xuất phát từ hoạt động truy cập trái phép, sử dụng, tiết lộ, làm suy giảm, gián đoạn, chỉnh sửa hoặc phá hoại thông tin, hệ thống thông tin.

20. *Chỉ báo về nguy cơ đe dọa an ninh mạng* là thông tin cần thiết để mô tả hoặc xác định:

a) Hoạt động xâm phạm chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng;

b) Mức độ độc hại hoặc các dấu hiệu bất thường tồn tại trên hệ thống thông tin hoặc đối với thông tin được lưu trữ, xử lý trên hệ thống thông tin;

c) Lỗ hổng bảo mật, phương pháp khai thác một lỗ hổng bảo mật hoặc phá vỡ sự kiểm soát an ninh;

d) Phương pháp tiếp cận bất hợp pháp vào một hệ thống thông tin hoặc thông tin được một hệ thống thông tin lưu trữ, xử lý trên hệ thống thông tin;

đ) Mạng botnet;

e) Thiệt hại an ninh mạng có thể xảy ra;

g) Các thông tin khác liên quan đến nguy cơ đe dọa an ninh mạng.

21. *Phương thức phòng thủ* *mạng* là hành động, biện pháp, thiết bị, dấu hiệu hoặc các phương thức khác được áp dụng cho hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền tải trong hệ thống thông tin nhằm phát hiện, phòng ngừa hoặc giảm thiểu các nguy cơ đe dọa an ninh mạng.

22. *Kiểm tra, đánh giá an ninh mạng* là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng không gian mạng 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.

23. *Kiểm soát an ninh mạng* là hoạt động quản lý kỹ thuật nhằm bảo vệ chủ quyền, lợi ích, an ninh quốc gia, thông tin, hệ thống thông tin, cơ sở hạ tầng không gian mạng nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng.

24. *Dữ liệu mạng* là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự được tạo ra, thu thập, lưu trữ, truyền tải, xử lý thông qua không gian mạng.

25. *Sự cố an ninh mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

26. *Lực lượng bảo vệ an ninh mạng,* bao gồm: lực lượng An ninh mạng thuộc Bộ Công an; lực lượng Tác chiến Không gian mạng thuộc Bộ Quốc phòng; lực lượng An toàn thông tin mạng thuộc Bộ Thông tin và Truyền thông; lực lượng Cơ yếu và các cơ quan, tổ chức, cá nhân khác được huy động thực hiện nhiệm vụ bảo vệ an ninh mạng khi có yêu cầu.

### Điều 4. Chính sách an ninh mạng

1. Bảo vệ an ninh mạng gắn liền với phát triển kinh tế, xã hội, quốc phòng, an ninh của đất nước.

2. Áp dụng mọi biện pháp giám sát, phòng chống và xử lý các nguy cơ đe dọa an ninh mạng, bảo vệ chủ quyền, lợi ích, an ninh quốc gia trước các cuộc tấn công, xâm nhập, phá hoại và các hoạt động bất hợp pháp khác theo quy định của pháp luật.

3. Xây dựng không gian mạng ổn định, lành mạnh. Các hành vi trên không gian mạng được ứng xử theo quy tắc, khuyến khích các hoạt động trung thực và văn minh trên không gian mạng, xử lý nghiêm minh các hành vi vi phạm theo quy định của pháp luật.

4. Bảo vệ quyền và lợi ích hợp pháp của tổ chức, công dân khi tham gia hoạt động trên không gian mạng theo pháp luật.

5. Thực hiện hợp tác quốc tế về an ninh mạng, góp phần bảo vệ không gian mạng hòa bình và minh bạch.

6. Ưu tiên bảo đảm kinh phí phục vụ công tác an ninh mạng.

### Điều 5. Nguyên tắc bảo vệ an ninh mạng

1. Mọi hoạt động bảo vệ an ninh mạng phải tuân thủ Hiến pháp, pháp luật, bảo đảm lợi ích Nhà nước, quyền và lợi ích hợp pháp của tổ chức, công dân.

2. Bảo vệ an ninh mạng là trách nhiệm của mọi cơ quan, tổ chức, công dân. Huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của các lực lượng công an, quân đội, thông tin và truyền thông, tuyên giáo, cơ yếu; đề cao trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, internet và cơ quan chủ quản hệ thống thông tin.

3. Chủ động phòng ngừa, chủ động đấu tranh làm thất bại mọi âm mưu và hoạt động sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội; sẵn sàng đáp trả các mối đe dọa chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

### Điều 6. Biện pháp bảo vệ an ninh mạng

1. Các biện pháp bảo vệ an ninh mạng bao gồm: các biện pháp bảo vệ an ninh quốc gia theo pháp luật về an ninh quốc gia, biện pháp nghiệp vụ an ninh mạng, biện pháp tác chiến trên không gian mạng và các biện pháp khác theo quy định của pháp luật.

2. Chính phủ quy định nội dung, điều kiện, thẩm quyền, trình tự, thủ tục và trách nhiệm áp dụng các biện pháp quy định tại khoản 1 Điều này.

### Điều 7. Các hành vi bị nghiêm cấm

1. Sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

2. Đăng tải 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.

3. Xâm nhập, chiếm đoạt trái phép thông tin, tài liệu.

4. Tấn công mạng.

5. Khủng bố mạng.

### Điều 8. Xử lý vi phạm pháp luật về an ninh mạng

Tổ chức, cá nhân nào vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

# *Chương II*

# BẢO VỆ AN NINH MẠNG

## Mục 1

## PHÒNG NGỪA, ĐẤU TRANH VỚI HOẠT ĐỘNG

## SỬ DỤNG KHÔNG GIAN MẠNG XÂM PHẠM AN NINH QUỐC GIA

### Điều 9. Xử lý thông tin kích động tụ tập đông người gây rối an ninh, trật tự trên không gian mạng

1. Kích động tụ tập đông người gây rối an ninh, trật tự trên không gian mạng là hành vi sử dụng không gian mạng đăng tải, truyền đưa, vận động, kêu gọi người dân tham gia tụ tập đông người gây rối an ninh, trật tự.

2. Các biện pháp xử lý thông tin kích động tụ tập đông người gây rối an ninh, trật tự trên không gian mạng:

a) Yêu cầu chủ thể đăng tải thông tin gỡ bỏ bài viết;

b) Ngăn chặn, xóa bỏ thông tin;

c) Tạm đình chỉ, đình chỉ hoặc rút giấp phép hoạt động của trang thông tin điện tử, cổng thông tin điện tử đăng tải thông tin;

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

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, internet có trách nhiệm phối hợp chặt chẽ với cơ quan chức năng xử lý thông tin kích động tụ tập đông người gây rối an ninh, trật tự trên không gian mạng.

### Điều 10. Xử lý thông tin 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

1. Nhà nước xây dựng không gian mạng lành mạnh; thực thi chính sách quản lý, ngăn chặn đăng tải, hiển thị, gỡ bỏ và xử lý trách nhiệm của người đăng tải thông tin chống Nhà nước, xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân, làm nhục, vu khống, vi phạm đạo đức, thuần phong mỹ tục trên không gian mạng theo quy định của pháp luật.

2. Nội dung thông tin 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:

a) Xuyên tạc sự thật lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết dân tộc;

b) Xuyên tạc, phỉ báng chính quyền nhân dân;

c) Bịa đặt, gây hoang mang trong nhân dân;

d) Gây chiến tranh tâm lý, kích động chiến tranh xâm lược, gây thù hận giữa các dân tộc và nhân dân các nước;

đ) Truyền bá tư tưởng phản động;

e) Xúc phạm dân tộc, danh nhân, anh hùng dân tộc;

g) Bịa đặt hoặc lan truyền, tán phát những điều biết rõ là sai sự thật nhằm xúc phạm nhân phẩm, danh dự hoặc làm nhục, vu khống tổ chức, cá nhân;

h) Hướng dẫn, xúi giục thực hiện các hành vi vi phạm pháp luật;

i) Thông tin xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân, trái đạo đức, thuần phong mỹ tục trên không gian mạng.

3. Xử lý thông tin 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:

a) Yêu cầu chủ thể đăng tải thông tin gỡ bỏ bài viết;

b) Ngăn chặn, xóa bỏ thông tin;

c) Tạm đình chỉ, đình chỉ hoặc rút giấp phép hoạt động của trang thông tin điện tử, cổng thông tin điện tử đăng tải thông tin;

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

4. Tổ chức, cá nhân tham gia hoạt động trên không gian mạng không được soạn thảo, đăng tải, lưu trữ, tán phát thông tin 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. Cơ quan chủ quản hệ thống thông tin, các doanh nghiệp cung cấp dịch vụ viễn thông, internet có trách nhiệm áp dụng biện pháp kỹ thuật để ngăn chặn hiển thị và xóa bỏ thông tin 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.

6. Bộ Công an chủ trì, phối hợp với Bộ Thông tin và Truyền thông áp dụng các biện pháp kỹ thuật và các biện pháp cần thiết khác để ngăn chặn việc lan truyền thông tin 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.

### Điều 11. Phòng, chống gián điệp mạng, bảo vệ thông tin, tài liệu thuộc bí mật nhà nước trên không gian mạng

1. Mọi hành vi cố ý xâm nhập vào hệ thống mạng thông tin hoặc phương tiện điện tử của cơ quan, tổ chức Nhà nước theo sự chỉ đạo của nước ngoài để chiếm đoạt bí mật nhà nước, thành tựu khoa học công nghệ, sở hữu trí tuệ hoặc hoạt động tình báo, phá hoại chống nước Cộng hòa xã hội chủ nghĩa Việt Nam đều bị xử lý nghiêm minh theo quy định về Tội gián điệp trong Bộ luật Hình sự.

2. Cơ quan soạn thảo, lưu trữ thông tin, tài liệu bí mật nhà nước có trách nhiệm:

a) Nghiêm cấm soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước trên máy tính kết nối internet hoặc các thiết bị khác có kết nối internet;

b) Kiểm tra, đánh giá an ninh mạng nhằm phát hiện, loại bỏ mã độc, khắc phục lỗ hổng bảo mật hoặc phát hiện, ngăn chặn các hoạt động xâm nhập bất hợp pháp;

c) Có kế hoạch để cán bộ, nhân viên tham gia các khóa 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 đảm an ninh mạng.

d) Phối hợp với Bộ Công an bảo vệ bí mật nhà nước trên không gian mạng và giám sát hệ thống thông tin nhằm phát hiện, xử lý hoạt động thu thập thông tin bí mật nhà nước;

đ) Phối hợp với Ban Cơ yếu Chính phủ bảo vệ bí mật nhà nước về cơ yếu.

3. Bộ Công an có trách nhiệm:

a) Kiểm tra, đánh giá an ninh mạng 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 cơ quan nhà nước;

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

c) Giám sát 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 pháp luật;

d) Phát hiện, xử lý các hành vi đăng tải thông tin, tài liệu có nội dung bí mật nhà nước trên mạng viễn thông, internet;

đ) Nghiên cứu, sản xuất các sản phẩm lưu trữ, truyền đưa thông tin, tài liệu bí mật nhà nước; các sản phẩm mã hóa bảo mật trên mạng viễn thông, internet;

e) Thanh tra, kiểm tra công tác bảo vệ an ninh mạng của cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia;

g) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo đảm 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.

4. Ban Cơ yếu Chính phủ có trách nhiệm:

a) Bảo vệ thông tin, bí mật nhà nước lưu trữ, trao đổi trên không gian mạng bằng mật mã;

b) Trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về mật mã trong lưu trữ, trao đổi thông tin bí mật nhà nước bằng mật mã trên không gian mạng.

### Điều 12. Phòng, chống tấn công mạng

1. Ngăn chặn, loại trừ hành vi tấn công mạng là trách nhiệm chung của toàn xã hội.

2. Xác định nguồn gốc tấn công mạng là xác định các thông tin liên quan đến gói tin như địa chỉ nguồn, địa chỉ đích, cổng dịch vụ… và cách thức, thủ đoạn, chủ thể thực hiện tấn công mạng. Căn cứ chức năng, nhiệm vụ, quyền hạn, trách nhiệm của mình, cơ quan, tổ chức, cá nhân áp dụng các biện pháp xác định nguồn gốc tấn công mạng phù hợp với quy định của pháp luật.

3. Triển khai các biện pháp giám sát an ninh mạng, phương thức phòng thủ mạng để phát hiện các hành vi:

a) Gây cản trở, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, internet, phương tiện điện tử[[1]](#footnote-2);

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

c) Sử dụng mạng máy tính, mạng internet, mạng viễn thông, phương tiện điện tử của người khác để gây ảnh hưởng, thiệt hại về vật chất, tinh thần của cơ quan, tổ chức, cá nhân khác;

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

4. Cơ quan chủ quản hệ thống thông tin áp dụng các biện pháp được pháp luật cho phép nhằm phòng ngừa, loại trừ hành vi tấn công mạng vào hệ thống thông tin do mình quản lý, có trách nhiệm phối hợp với các cơ quan chuyên trách bảo vệ an ninh mạng để xác định chính xác nguồn gốc tấn công mạng.

5. Khi xuất hiện hoạt động tấn công mạng gây ảnh hưởng đến chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng, cơ quan chuyên trách bảo vệ an ninh mạng yêu cầu các doanh nghiệp cung cấp dịch vụ viễn thông, internet chặn lọc thông tin nhằm ngăn chặn, loại trừ hành vi tấn công mạng.

6. Cơ quan chuyên trách bảo vệ an ninh mạng áp dụng các biện pháp loại trừ tấn công mạng theo quy định của pháp luật.

7. 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 trên phạm vi cả nước; áp dụng các biện pháp bảo vệ an ninh mạng để phòng ngừa, phát hiện, xử lý hành vi tấn công mạng gây tổn hại đến chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

8. Bộ Quốc phòng chủ trì, phối hợp với bộ, ngành liên quan ngăn chặn, loại trừ các hành vi tấn công mạng của lực lượng quân sự nước ngoài gắn với chiến tranh xâm lược và các hành vi tấn công mạng gây tổn hại đến hệ thống thông tin quân sự, quốc phòng theo chức năng, nhiệm vụ được giao.

9. Bộ Thông tin và Truyền thông chủ trì, phối hợp với các bộ, ngành liên quan ngăn chặn hoạt động tấn công mạng gây mất an toàn thông tin mạng theo chức năng, nhiệm vụ được giao.

10. Ban cơ yếu Chính phủ chủ trì, phối hợp với các bộ, ngành liên quan phòng ngừa, đấu tranh với hành vi tấn công mạng vào hệ thống liên lạc cơ yếu.

### Điều 13. Phòng, chống khủng bố mạng

1. Nhà nước 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 khi phát hiện dấu hiệu, hành vi khủng bố mạng phải kịp thời báo cho 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 trao đổi cơ quan chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.

3. Khi có căn cứ xác định xảy ra, đã hoặc đang xảy ra khủng bố mạng, Bộ Công an chủ trì, phối hợp với các bộ, ngành triển khai công tác phòng, chống khủng bố mạng, không để khủng bố mạng hoặc hạn chế đến mức thấp nhất hậu quả xảy ra. Trường hợp cần thiết, áp dụng biện pháp vô hiệu hóa nguồn khủng bố mạng để loại trừ hành vi tấn công mạng.

4. Thường xuyên rà soát, kiểm tra, đánh giá an ninh mạng nhằm loại trừ nguy cơ khủng bố mạng.

### Điều 14. Phòng, chống chiến tranh mạng

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

2. Bảo đảm tính sẵn sàng chiến đấu của hệ thống thông tin quân sự, chủ động đối phó với chiến tranh mạng và thách thức do chiến tranh mạng đặt ra, loại bỏ nguy cơ chiến tranh mạng.

3. Khi có khả năng xảy ra hoặc xảy ra chiến tranh mạng, cơ quan, tổ chức, cá nhân chủ động áp dụng các biện pháp bảo vệ an ninh mạng, bảo vệ hệ thống thông tin do mình quản lý theo chức năng, nhiệm vụ, thẩm quyền, trách nhiệm được giao.

4. Bộ Quốc phòng chủ trì phòng, chống chiến tranh mạng; chủ trì, phối hợp với Bộ Công an và các bộ, ngành liên quan áp dụng biện pháp tương xứng, phù hợp.

### Điều 15. Tình huống khẩn cấp về an ninh mạng

1. Khi xảy ra các tình huống sau đây, Thủ tướng Chính phủ xem xét, quyết định hoặc giao Bộ trưởng Bộ Công an xem xét, quyết định tình huống khẩn cấp về an ninh mạng trong cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể:

a) Tấn công cục bộ hệ thống thông tin quan trọng về an ninh quốc gia[[2]](#footnote-3);

b) Tấn công diện rộng hệ thống thông tin quan trọng về an ninh quốc gia[[3]](#footnote-4);

c) Tấn công trên quy mô lớn, cường độ cao vào hệ thống thông tin quốc gia;

d) Tấn công mạng nhằm phá hủy công trình trọng yếu quốc gia, mục tiêu quan trọng về an ninh quốc gia hoặc nhằm gây thiệt hại về sinh mạng, tài sản[[4]](#footnote-5);

đ) Chiến tranh thông tin;

e) Khi xảy ra 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, quyền và lợi ích hợp pháp của nhiều tổ chức, cá nhân;

g) Khi có yêu cầu đột xuất, cấp bách vì lý do bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm phối hợp với Bộ Công an thực hiện các biện pháp nhằm ngăn chặn, xử lý tình huống khẩn cấp về an ninh mạng.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan xử lý tình huống khẩn cấp về an ninh mạng, áp dụng đồng bộ các biện pháp theo quy định của pháp luật để ngăn chặn, xử lý.

### Điều 16. Các biện pháp áp dụng khi gia tăng nguy cơ xảy ra tình huống khẩn cấp về an ninh mạng

1. Khi gia tăng nguy cơ xảy ra tình huống khẩn cấp về an ninh mạng, Bộ Công an chủ trì, phối hợp với các bộ, ngành và ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương thực hiện các biện pháp sau:

a) Yêu cầu các cơ quan, tổ chức và cá nhân liên quan kịp thời thu thập, báo cáo các thông tin liên quan, tăng cường giám sát đối với sự cố an ninh mạng;

b) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ gây hại của sự cố an ninh mạng;

c) Thông báo tới cơ quan, tổ chức, cá nhân có liên quan;

d) Áp dụng phương án phòng ngừa, ứng cứu khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do sự cố an ninh mạng gây ra;

đ) Bảo đảm lực lượng, phương tiện tham gia ngăn chặn, loại bỏ nguy cơ xảy ra tình huống khẩn cấp về an ninh mạng.

2. Khi thực hiện chức năng quản lý nhà nước về viễn thông, internet, nếu phát hiện các nguy cơ đe dọa an ninh mạng có khả năng xảy ra hậu quả, thiệt hại nghiêm trọng hoặc nguy cơ xảy ra tình huống khẩn cấp về an ninh mạng, các bộ, ngành, địa phương kịp thời thông báo về Bộ Công an và áp dụng các biện pháp được quy định tại Khoản 1 Điều này.

3. Các doanh nghiệp viễn thông, internet, công nghệ thông tin và tổ chức, cá nhân liên quan có trách nhiệm phối hợp với Bộ Công an trong phòng ngừa, xử lý tình huống khẩn cấp về an ninh mạng.

### Điều 17. Bảo đảm nguồn lực bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng

1. Công dân Việt Nam có trình độ về công nghệ thông tin, an toàn thông tin mạng, an ninh mạng là nguồn lực cơ bản, chủ yếu bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

2. Nhà nước có chính sách, kế hoạch xây dựng, bồi dưỡng nguồn nhân lực bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

3. Khi xảy ra tình huống khẩn cấp về an ninh mạng hoặc khi có yêu cầu đột xuất, cấp bách vì lý do bảo vệ chủ quyền, lợi ích, an ninh quốc gia, Nhà nước quyết định 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 theo quy định của pháp luật.

## Mục 2

## BẢO VỆ HỆ THỐNG THÔNG TIN QUAN TRỌNG

## VỀ AN NINH QUỐC GIA

### Điều 18. Hệ thống thông tin quan trọng về an ninh quốc gia

1. Tiêu chí xác định hệ thống thông tin quan trọng về an ninh quốc gia

Hệ thống thông tin quan trọng về an ninh quốc gia được xác định theo tính chất quan trọng đối với an ninh quốc gia, trật tự an toàn xã hội của hệ thống thông tin và mức độ hậu quả, thiệt hại có thể xảy ra khi hệ thống thông tin bị xâm hại:

a) Gây ảnh hưởng đến chủ quyền, lợi ích, an ninh quốc gia.

b) Gây ảnh hưởng nghiêm trọng đến trật tự an toàn xã hội.

2. Hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm:

a) Hệ thống thông tin phục vụ bảo vệ an ninh quốc gia;

b) Hệ thống thông tin xử lý thông tin bí mật nhà nước;

c) Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử;

d) Hệ thống thông tin của các ngành, lĩnh vực trọng yếu quốc gia, gồm: hóa chất, thương mại, thông tin, hệ thống đập nước, căn cứ công nghiệp quốc phòng, các dịch vụ khẩn cấp, năng lượng, tài chính, nông nghiệp và thực phẩm, y tế và chăm sóc sức khỏe, công nghệ thông tin, vật liệu và lò phản ứng hạt nhân, các hệ thống vận tải, các hệ thống cấp thoát nước;

đ) Hệ thống điều khiển và giám sát tự động tại các công trình trọng yếu quốc gia, mục tiêu quan trọng về an ninh quốc gia;

e) Hệ thống thông tin phục vụ phát thanh, truyền hình, báo chí, xuất bản;

g) Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một loại hình thông tin, dữ liệu đặc biệt quan trọng quốc gia;

h) Hệ thống cơ sở hạ tầng thông tin quốc gia phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.

### Điều 19. Nguyên tắc bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia

1. Hệ thống thông tin quan trọng về an ninh quốc gia có vai trò đặc biệt quan trọng đối với quốc phòng, an ninh, nền kinh tế, chính trị, xã hội và sự phát triển của đất nước, phải được bảo vệ nghiêm ngặt.

2. Bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia là trách nhiệm của hệ thống chính trị và toàn xã hội, trước hết là của cơ quan chủ quản.

Các cơ quan, tổ chức, cá nhân tuân thủ nghiêm các quy định của pháp luật, áp dụng các tiêu chuẩn, biện pháp cần thiết để bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia theo nguyên tắc kiểm tra, đánh giá trước, sử dụng sau.

3. Bộ Công an cung cấp các biện pháp, điều kiện bảo đảm an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: xây dựng các tiêu chuẩn chung về bảo vệ an ninh mạng; kiểm tra, đánh giá, thẩm định, cấp chứng nhận hợp chuẩn an ninh mạng; giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; tổ chức diễn tập an ninh mạng và đào tạo, bồi dưỡng kỹ năng bảo vệ an ninh mạng; ứng cứu, khắc phục sự cố thông qua hợp tác, trao đổi và điều phối với các cơ quan liên quan; chia sẻ thông tin an ninh mạng giữa các cơ quan hành chính quốc gia, các tổ chức, doanh nghiệp.

### Điều 20. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Hệ thống thông tin quan trọng về an ninh quốc gia phải thẩm định khả năng bảo đảm an ninh mạng:

a) Trước khi hệ thống thông tin quan trọng về an ninh quốc gia được đưa vào vận hành, sử dụng;

b) Trước khi đưa sản phẩm, dịch vụ mạng vào hệ thống thông tin quan trọng về an ninh quốc gia.

c) Khi có yêu cầu quản lý nhà nước về an ninh mạng.

2. Cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia:

a) Khi mua các sản phẩm, dịch vụ mạng phải yêu cầu doanh nghiệp cung cấp cam kết về khả năng bảo đảm an ninh mạng;

b) Giao sản phẩm, dịch vụ mạng được nêu tại Điểm a, Khoản 2 Điều này cho cơ quan chuyên trách bảo vệ an ninh mạng của Bộ Công an hoặc tổ chức chuyên môn được Bộ Công an chỉ định thẩm định.

3. Bộ Công an thẩm định hoặc chỉ định tổ chức chuyên môn được cơ quan nhà nước có thẩm quyền công nhận thẩm định an ninh mạng của các sản phẩm, dịch vụ mạng trước khi đưa vào sử dụng tại hệ thống thông tin quan trọng về an ninh quốc gia.

### Điều 21. Kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Kiểm tra, đánh giá ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, phòng ngừa, loại bỏ các mối đe dọa an ninh mạng vào các nguồn tài nguyên thông tin và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin quan trọng về an ninh quốc gia.

2. Kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia trên cơ sở:

a) Phân tích dữ liệu thu được khi sử dụng các phương tiện kỹ thuật kiểm tra hệ thống thông tin, bao gồm cả thông tin về các dấu hiệu tấn công vào hệ thống thông tin.

b) Các tài liệu thu được thông qua hoạt động quản lý nhà nước trong lĩnh vực an ninh mạng;

c) Các thông tin khác phù hợp với pháp luật nước Cộng hòa xã hội chủ nghĩa Việt Nam.

3. Bộ Công an triển khai các giải pháp kỹ thuật, nghiệp vụ tại các hệ thống thông tin quan trọng về an ninh quốc gia nhằm phòng ngừa, phát hiện, xử lý các hoạt động tấn công, xâm nhập.

### Điều 22. Giám sát, cảnh báo, ứng cứu, khắc phục sự cố xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia

1. Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện thường xuyên, liên tục nhằm phòng ngừa, phát hiện các mối đe dọa an ninh mạng và khắc phục các điểm yếu, lỗ hổng bảo mật, loại bỏ mã độc tồn tại trong hệ thống thông tin.

2. Cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm xây dựng cơ chế cảnh báo các mối đe dọa an ninh mạng, đề ra phương án ứng cứu, khắc phục khẩn cấp sự cố xảy ra đối với hệ thống thông tin của đơn vị mình.

3. Khi xảy ra sự cố, cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải kịp thời thông báo và phối hợp với Bộ Công an:

a) Thu thập, báo cáo thông tin liên quan, tăng cường giám sát tình hình sự cố;

b) Phân tích, đánh giá, dự đoán khả năng phát sinh, phạm vi ảnh hưởng, mức độ nguy hại;

c) Tổ chức ứng cứu, khắc phục.

4. Bộ trưởng Bộ Công an thông báo tình hình liên quan đến sự cố an ninh mạng; tạm thời hạn chế hoạt động của hệ thống thông tin tại một số khu vực khi thấy cần thiết.

5. Bộ Công an có trách nhiệm:

a) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, ngoại trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý;

b) Chủ trì, phối hợp với Bộ Thông tin và Truyền thông, Bộ Quốc phòng trong huy động lực lượng, cơ sở vật chất kỹ thuật ứng cứu, khắc phục sự cố xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia;

c) Phối hợp với Ban Cơ yếu Chính phủ giám sát an ninh mạng với hệ thống mạng liên lạc cơ yếu do Ban Cơ yếu Chính phủ quản lý.

## Mục 3

## GIÁM SÁT, DỰ BÁO, ỨNG CỨU

## VÀ DIỄN TẬP ỨNG CỨU SỰ CỐ AN NINH MẠNG

### Điều 23. Giám sát an ninh mạng

1. Giám sát an ninh mạng là hoạt động thu thập, nhận biết, rà quét, xử lý thông tin một cách có hệ thống nhằm xác định những nhân tố gây ảnh hưởng đến an ninh mạng hoặc có khả năng gây ra sự cố an ninh mạng.

2. Đối tượng giám sát an ninh mạng gồm hệ thống tường lửa, kiểm soát truy nhập, truyền thông tin chủ yếu, kiểm soát lưu lượng mạng, máy chủ quan trọng, thiết bị quan trọng hoặc thiết bị đầu cuối.

3. Chính phủ quy định cụ thể về giám sát an ninh mạng.

### Điều 24. Dự báo an ninh mạng

1. Dự báo an ninh mạng là hoạt động khoa học trên cơ sở phân tích, xử lý số liệu, dữ liệu mạng thu được để xác định xu hướng vận động của an ninh mạng.

2. Quy trình dự báo an ninh mạng

a) Xác định mục tiêu dự báo;

b) Xác định nội dung dự báo an ninh mạng: bảo mật (lộ, lọt, chiếm đoạt bí mật nhà nước, xâm nhập hệ thống thông tin); tấn công mạng, khủng bố mạng; chiến tranh mạng; sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội;

c) Chọn mô hình dự báo;

d) Thu thập số liệu và tiến hành dự báo;

đ) Ứng dụng kết quả dự báo, lập kế hoạch phòng ngừa, ứng phó;

e) Theo dõi, đánh giá kết quả dự báo.

3. Bộ Công an chủ trì, phối hợp với bộ, ngành liên quan nghiên cứu, phân tích tình hình, dự báo xu hướng an ninh mạng và lập kế hoạch phòng ngừa, ứng phó với sự cố an ninh mạng.

4. Tùy từng trường hợp cụ thể, cơ quan chuyên trách bảo vệ an ninh mạng gửi dự báo của mình tới các tổ chức, cá nhân trong và ngoài nước.

### Điều 25. Ứng cứu, khắc phục sự cố an ninh mạng

1. Ứng cứu, khắc phục sự cố an ninh mạng là trách nhiệm của cơ quan chủ quản hệ thống thông tin.

2. Cơ quan, tổ chức, cá nhân xây dựng các phương án ứng cứu, khắc phục sự cố an ninh mạng đối với hệ thống thông tin do mình quản lý; chủ động ký hợp đồng với các tổ chức chuyên môn được cấp giấy phép thực hiện dịch vụ ứng cứu, khắc phục sự cố an ninh mạng theo quy định tại Điều 32, 33, 34, 35 Luật này;

3. Các bộ, ngành, địa phương, cơ quan nhà nước thành lập hoặc chỉ định bộ phận chuyên trách ứng cứu, khắc phục sự cố an ninh mạng.

4. Bộ Công an có trách nhiệm:

a) Điều phối hoạt động ứng cứu, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia; khi xảy ra tình huống khẩn cấp về an ninh mạng; sự cố an ninh mạng xảy ra gây ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia trên phạm vi cả nước;

b) Tham gia ứng cứu, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu; chi phí ứng cứu, khắc phục sự cố do cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia chi trả;

c) Tổ chức diễn tập ứng cứu, khắc phục sự cố an ninh mạng.

### Điều 26. Diễn tập ứng cứu sự cố an ninh mạng

1. Hằng năm, Bộ Công an chủ trì, phối hợp với các bộ, ngành chức năng, các cơ quan, tổ chức trong và ngoài nước diễn tập ứng cứu sự cố an ninh mạng.

2. Phương án diễn tập ứng cứu sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm phương án tổng thể và phương án cụ thể áp dụng với từng hệ thống thông tin riêng lẻ.

3. Kết quả công tác diễn tập ứng cứu sự cố an ninh mạng là căn cứ để đánh giá tình trạng nhân lực bảo vệ an ninh mạng, mức độ sẵn sàng và hiệu quả của phương án ứng cứu sự cố an ninh mạng.

### Điều 27. Ngừng cung cấp thông tin mạng

Trường hợp cần thiết, Bộ Công an đề xuất Chính phủ ngừng cung cấp thông tin mạng tại các khu vực cụ thể để ứng phó, khắc phục các sự cố an ninh mạng để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội.

## Mục 4

## TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN NINH MẠNG

## VÀ CẤP PHÉP KINH DOANH DỊCH VỤ BẢO ĐẢM AN NINH MẠNG

### Điều 28. Xây dựng tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng

1. Nhà nước khuyến khích cơ quan, tổ chức, cá nhân xây dựng và ban hành tiêu chuẩn về an ninh mạng, chỉ định cơ quan quản lý nhà nước về an ninh mạng xây dựng quy chuẩn kỹ thuật an ninh mạng đối với các lĩnh vực cụ thể trong công tác an ninh mạng.

2. Bộ Công an chủ trì, phối hợp xây dựng, đề nghị thẩm định dự thảo tiêu chuẩn quốc gia về an ninh mạng; xây dựng, đề nghị thẩm định, công bố, ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng, quy định về đánh giá hợp quy về an ninh mạng.

3. Bộ Khoa học và Công nghệ chủ trì, phối hợp với cơ quan có liên quan tổ chức thẩm định và công bố tiêu chuẩn quốc gia về an ninh mạng theo quy định của pháp luật.

4. Nhà nước khuyến khích các cơ quan, doanh nghiệp, tổ chức, ngành nghề liên quan công nghệ thông tin, viễn thông, internet tham gia xây dựng tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng.

### Điều 29. Chứng nhận, công bố hợp chuẩn, hợp quy về an ninh mạng

1. Chứng nhận, công bố hợp chuẩn về an ninh mạng:

a) Chứng nhận hợp chuẩn về an ninh mạng là việc tổ chức chứng nhận sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành hệ thống thông tin phù hợp với tiêu chuẩn an ninh mạng;

b) Công bố hợp chuẩn về an ninh mạng là việc tổ chức, doanh nghiệp công bố sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành hệ thống thông tin phù hợp với tiêu chuẩn an ninh mạng.

2. Chứng nhận, công bố hợp quy về an ninh mạng:

a) Chứng nhận hợp quy về an ninh mạng là việc tổ chức chứng nhận sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành hệ thống thông tin phù hợp với quy chuẩn kỹ thuật về an ninh mạng;

b) Công bố hợp quy về an ninh mạng là việc tổ chức, doanh nghiệp công bố sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng phù hợp với quy chuẩn kỹ thuật về an ninh mạng;

3. Bộ Công an có trách nhiệm:

a) Đăng ký, chỉ định và quản lý hoạt động của tổ chức đánh giá chứng nhận hợp chuẩn, hợp quy về an ninh mạng;

b) Thông báo bằng văn bản tới cơ quan chủ quản hệ thống thông tin quan trọng quốc gia khi hệ thống thông tin quan trọng về an ninh quốc gia do cơ quan này quản lý, vận hành không đáp ứng được các quy chuẩn kỹ thuật về an ninh mạng;

c) Đề xuất hình thức xử lý đối với cá nhân có liên quan khi hệ thống thông tin quan trọng về an ninh quốc gia không đáp ứng được các quy chuẩn kỹ thuật về an ninh mạng để xảy ra sự cố;

d) Trường hợp khẩn cấp, đề xuất Chính phủ ra Quyết định đình chỉ hoặc tạm đình chỉ hệ thống thông tin quan trọng về an ninh quốc gia để khắc phục, xử lý.

### Điều 30. Đánh giá hợp chuẩn, hợp quy về an ninh mạng

1. Việc đánh giá hợp chuẩn, hợp quy về an ninh mạng được thực hiện trong các trường hợp sau đây:

a) Trước khi tổ chức, cá nhân đưa sản phẩm an ninh mạng vào lưu thông trên thị trường;

b) Trước khi đưa hệ thống thông tin quan trọng về an ninh quốc gia vào hoạt động hoặc đưa sản phẩm, thiết bị vào hệ thống thông tin quan trọng về an ninh quốc gia;

c) Phục vụ hoạt động quản lý nhà nước về an ninh mạng.

2. Việc đánh giá, chứng nhận hợp chuẩn, hợp quy về an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia và phục vụ hoạt động quản lý nhà nước về an ninh mạng được thực hiện tại tổ chức chứng nhận sự phù hợp do Bộ Công an chỉ định;

3. Cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp, chấp hành các yêu cầu của Bộ Công an trong đánh giá hợp quy về an ninh mạng.

4. Việc thừa nhận kết quả đánh giá hợp chuẩn, hợp quy về an ninh mạng giữa Việt Nam với quốc gia, vùng lãnh thổ khác, giữa tổ chức chứng nhận sự phù hợp của Việt Nam với tổ chức chứng nhận sự phù hợp của quốc gia, vùng lãnh thổ khác được thực hiện theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

### Điều 31. Yêu cầu bảo đảm an ninh mạng trong sản xuất, kinh doanh sản phẩm, dịch vụ mạng

1. Yêu cầu bảo đảm an ninh mạng đối với sản phẩm, dịch vụ mạng

a) Bảo đảm các sản phẩm, dịch vụ mạng không cài đặt chương trình độc hại;

b) Kiểm tra chất lượng trước khi cung cấp ra thị trường, trước khi sử dụng nhằm xác định, loại bỏ những nội dung, yếu tố không bảo đảm an ninh mạng;

c) Chất lượng sản phẩm, dịch vụ mạng phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng công bố áp dụng tương ứng;

d) Áp dụng các biện pháp khắc phục hậu quả, kịp thời thông báo đến người dùng và báo cáo cơ quan quản lý nhà nước liên quan khi phát hiện sản phẩm, dịch vụ mạng tồn tại lỗi, lỗ hổng bảo mật;

đ) Sản phẩm, dịch vụ mạng có chức năng thu thập thông tin người dùng phải thể hiện, thông báo rõ để người dùng biết và phải được sự đồng ý của người dùng.

2. Sản phẩm, dịch vụ mạng sử dụng trong cơ quan, tổ chức có bí mật nhà nước, hệ thống thông tin quan trọng về an ninh quốc gia, phục vụ lãnh đạo Nhà nước phải phù hợp với yêu cầu, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật về an ninh mạng đối với sản phẩm, dịch vụ mạng và chỉ được bán, cung cấp, sử dụng sau khi bảo đảm yêu cầu và đáp ứng tiêu chuẩn chứng nhận hợp chuẩn, hợp quy về an ninh mạng của cơ quan có thẩm quyền.

### Điều 32. Dịch vụ bảo đảm an ninh mạng

1. Dịch vụ bảo đảm an ninh mạng bao gồm:

a) Dịch vụ kiểm tra, đánh giá an ninh mạng (Security Audit): Kiểm tra, đánh giá an ninh hệ thống để bảo đảm các phương pháp an ninh, an toàn thông tin và hệ thống vẫn hoạt động hiệu quả, đúng mục đích sử dụng;

b) Dịch vụ tư vấn an ninh mạng:

- Tư vấn thiết kế bảo đảm an ninh cho các hệ thống mạng; quy hoạch lại hệ thống cũ bảo đảm hiệu năng an ninh; thiết kế xây dựng hệ thống mạng mới;

- Tư vấn thiết lập hệ thống quản lý an ninh mạng: các yêu cầu trong xây dựng, áp dụng, điều hành, kiểm tra, giám sát và phát triển hệ thống quản lý an ninh mạng một cách đầy đủ, khoa học.

c) Dịch vụ giám sát an ninh mạng;

d) Dịch vụ ứng cứu, khắc phục sự cố an ninh mạng;

đ) Dịch vụ phòng, chống tấn công mạng;

e) Dịch vụ kiểm tra, thử nghiệm (pentest): Kiểm tra khả năng bảo đảm an ninh mạng của hệ thống thông tin bằng cách giả lập các vụ tấn công thử nghiệm.

2. Các dịch vụ an toàn thông tin mạng được quy định tại Khoản 1 Điều 41 Luật An toàn thông tin mạng nếu có trùng về nội dung với dịch vụ bảo đảm an ninh mạng được quy định tại Khoản 2 Điều này thì ưu tiên xác định, áp dụng theo quy định tại Luật này.

3. Bộ Công an chủ trì, phối hợp với Bộ Công thương bổ sung kinh doanh dịch vụ bảo đảm an ninh mạng vào Phụ lục: Danh mục ngành, nghề kinh doanh có điều kiện theo quy định của pháp luật về đầu tư.

### Điều 33. Điều kiện cấp giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng

1. Người đứng đầu cơ sở kinh doanh dịch vụ bảo đảm an ninh mạng phải có lý lịch rõ ràng và không thuộc một trong các trường hợp sau:

a) Người chưa thành niên, người bị hạn chế hoặc mất năng lực hành vi dân sự;

b) Người bị khởi tố hình sự mà các cơ quan tố tụng đang tiến hành điều tra, truy tố, xét xử;

c) Người đang bị tòa án cấm đảm nhiệm chức vụ, cấm hành nghề có liên quan.

2. Cơ sở kinh doanh dịch vụ bảo đảm an ninh mạng:

- Đáp ứng tiêu chuẩn số lượng về đội ngũ nhân viên kỹ thuật có bằng đại học chuyên ngành hoặc chứng chỉ an ninh mạng, công nghệ thông tin, viễn thông;

- Có mô tả về phương án kinh doanh dịch vụ bảo đảm an ninh mạng phù hợp với quy định của pháp luật;

- Có hệ thống trang thiết bị, cơ sở vật chất và công nghệ phù hợp với mô tả về phương án kinh doanh dịch vụ an ninh mạng.

### Điều 34. Hồ sơ đề nghị cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng

1. Cơ sở đề nghị cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng nộp hồ sơ đề nghị cấp Giấy phép tại Bộ Công an.

2. Hồ sơ đề nghị cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng, gồm:

a) Đơn đề nghị cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng;

b) Bản sao Giấy chứng nhận đăng ký doanh nghiệp, Giấy chứng nhận đăng ký đầu tư hoặc giấy tờ khác có giá trị tương đương;

c) Bản thuyết minh hệ thống thiết bị kỹ thuật bảo đảm phù hợp với quy định của pháp luật;

d) Bản mô tả phương án kinh doanh gồm phạm vi, đối tượng cung cấp dịch vụ, tiêu chuẩn, chất lượng dịch vụ;

đ) Bản sao văn bằng hoặc chứng chỉ chuyên môn về an ninh mạng, công nghệ thông tin, viễn thông của đội ngũ quản lý, điều hành, kỹ thuật bảo đảm theo tiêu chuẩn số lượng tương ứng.

### Điều 35. Thẩm định hồ sơ và cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng

1. Trong thời hạn 20 ngày kể từ ngày nhận đủ hồ sơ, Bộ Công an chủ trì, phối hợp với bộ, ngành có liên quan thẩm định và cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

2. Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng có nội dung chính sau đây:

a) Tên doanh nghiệp, tên giao dịch của cơ sở kinh doanh bằng tiếng Việt và tiếng nước ngoài (nếu có); địa chỉ trụ sở chính tại Việt Nam;

b) Tên của người đại diện theo pháp luật;

c) Số giấy phép, ngày cấp giấy phép, ngày hết hạn giấy phép;

d) Dịch vụ an ninh mạng được phép kinh doanh.

3. Cơ sở kinh doanh được cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng phải nộp phí theo quy định của pháp luật về phí và lệ phí.

### Điều 36. Sửa đổi, bổ sung, gia hạn, tạm đình chỉ, thu hồi và cấp lại Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng

1. Việc sửa đổi, bổ sung Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng được thực hiện trong trường hợp doanh nghiệp đã được cấp Giấy phép thay đổi tên, thay đổi người đại diện theo pháp luật hoặc thay đổi, bổ sung dịch vụ bảo đảm an ninh mạng mà mình cung cấp.

Cơ sở kinh doanh có trách nhiệm nộp hồ sơ đề nghị sửa đổi, bổ sung nội dung Giấy phép tại Bộ Công an. Hồ sơ được lập thành hai bộ, gồm đơn đề nghị sửa đổi, bổ sung nội dung Giấy phép, báo cáo mô tả chi tiết nội dung đề nghị sửa đổi, bổ sung và các tài liệu khác có liên quan.

Trong thời hạn 10 ngày làm việc kể từ ngày nhận đủ hồ sơ, Bộ Công an thẩm định, sửa đổi, bổ sung và cấp lại Giấy phép cho doanh nghiệp; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

2. Trường hợp Giấy phép kinh doanh dịch vụ an ninh mạng bị mất hoặc bị hư hỏng, cơ sở kinh doanh gửi đơn đề nghị cấp lại Giấy phép tới Bộ Công an, trong đơn nêu rõ lý do. Trong thời hạn 05 ngày làm việc kể từ ngày nhận được đơn đề nghị, Bộ Công an xem xét và cấp lại Giấy phép cho cơ sở kinh doanh.

3. Cơ sở kinh doanh không vi phạm quy định của pháp luật về kinh doanh dịch vụ bảo đảm an ninh mạng được gia hạn Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng một lần với thời gian gia hạn không quá 01 năm. Hồ sơ đề nghị gia hạn Giấy phép phải được gửi tới Bộ Công an chậm nhất là 60 ngày trước ngày Giấy phép hết hạn. Hồ sơ đề nghị gia hạn Giấy phép được lập thành hai bộ, gồm:

a) Đơn đề nghị gia hạn Giấy phép;

b) Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng đang có hiệu lực;

c) Báo cáo hoạt động của doanh nghiệp trong 02 năm gần nhất.

Trong thời hạn 20 ngày kể từ ngày nhận đủ hồ sơ, Bộ Công an thẩm định, quyết định gia hạn và cấp lại Giấy phép cho cơ sở kinh doanh; trường hợp từ chối cấp thì phải thông báo bằng văn bản và nêu rõ lý do.

4. Cơ sở kinh doanh bị tạm đình chỉ hoạt động kinh doanh dịch vụ bảo đảm an ninh mạng có thời hạn không quá 06 tháng trong các trường hợp sau đây:

a) Cung cấp dịch vụ không đúng với nội dung ghi trên Giấy phép;

b) Không đáp ứng được một trong các điều kiện quy định tại Điều 42 của Luật này;

c) Các trường hợp khác theo quy định của pháp luật.

5. Cơ sở kinh doanh bị thu hồi Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng trong các trường hợp sau đây:

a) Không triển khai cung cấp dịch vụ trong thời hạn 01 năm kể từ ngày được cấp Giấy phép mà không có lý do chính đáng;

b) Giấy phép đã hết hạn;

c) Hết thời hạn tạm đình chỉ mà cơ sở kinh doanh không khắc phục được các lý do quy định tại khoản 4 Điều này.

# *Chương III*

# TRIỂN KHAI CÔNG TÁC AN NINH MẠNG

### Điều 37. Triển khai công tác an ninh mạng trong hệ thống cơ quan nhà nước

1. Chính phủ triển khai công tác bảo vệ an ninh mạng từ Trung ương đến địa phương thông qua phân công lực lượng thực hiện nhiệm vụ bảo đảm an ninh mạng, gắn liền với quá trình ứng dụng công nghệ thông tin và triển khai Chính phủ điện tử; khuyến khích khu vực tư nhân tham gia công tác bảo vệ an ninh mạng, nghiên cứu, phát triển sản phẩm, dịch vụ bảo vệ an ninh mạng.

2. Các bộ, ngành và UBND các tỉnh, thành phố trực thuộc quy hoạch thống nhất, tăng cường đầu tư, hỗ trợ các hạng mục, sản xuất kỹ thuật an ninh mạng trọng điểm; khuyến khích nghiên cứu, phát triển và ứng dụng kỹ thuật an ninh mạng; quảng bá sản phẩm, dịch vụ mạng an toàn, đáng tin cậy; bảo vệ quyền sở hữu trí tuệ kỹ thuật mạng, ủng hộ doanh nghiệp, tổ chức nghiên cứu, các trường đại học, cao đẳng… tham gia vào dự án, hạng mục nghiên cứu, sáng tạo kỹ thuật an ninh mạng.

3. Bộ Công an nghiên cứu, phân công lực lượng an ninh mạng chuyên trách trực thuộc và tại Công an các tỉnh, thành phố trực thuộc Trung ương.

### Điều 38. Nghiên cứu chiến lược phát triển và bảo vệ an ninh mạng

1. Nội dung nghiên cứu chiến lược phát triển và bảo vệ an ninh mạng:

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, không 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 được nêu và chỉ có chức năng đó;

d) Phương pháp bảo vệ bí mật nhà nước, 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.

2. Xây dựng thao trường mạng dựa trên đề xuất của Bộ Công an tạo môi trường thử nghiệm an ninh mạng đủ mạnh để mô hình quá hóa quy mô và độ phức tạp của các cuộc tấn công mạng thời gian thực và những phương thức phòng thủ trong môi trường và hệ thống mạng thế giới thực.

3. Việc nghiên cứu chiến lược phát triển và bảo vệ an ninh mạng được thực hiện bởi:

a) Bộ Công an;

b) Bộ Khoa học và công nghệ;

c) Các bộ, ngành chức năng;

d) Các Phòng thí nghiệm nghiên cứu của nhà nước và tư nhân;

đ) Cơ sở đào tạo, tổ chức giáo dục;

e) Các tổ chức phi lợi nhuận có liên quan;

g) Các đối tác quốc tế của Việt Nam.

4. Lĩnh vực được tài trợ trong nghiên cứu chiến lược phát triển và bảo vệ an ninh mạng:

a) Các giao thức cơ bản bảo mật cần thiết phục vụ trao đổi dữ liệu, liên lạc mạng;

b) Ngôn ngữ và hệ thống lập trình đối với các tính năng bảo mật;

c) Mã di động hoặc tái sử dụng trong các môi trường khác nhau;

d) Công nghệ kiểm chứng và xác thực;

đ) Mô hình thử nghiệm an ninh mạng;

e) Khắc phục lỗ hổng bảo mật;

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

h) Tăng cường an ninh mạng và bảo vệ quyền riêng tư;

i) Phương pháp phục hồi dữ liệu;

k) Bảo mật hệ thống mạng không dây và thiết bị di động;

l) Bảo mật dịch vụ và cơ sở hạ tầng điện toán đám mây;

m) Dịch ngược mã nguồn;

n) Điều tra số.

5. Bộ Công an chủ trì nghiên cứu, phát triển và đề xuất Chính phủ chiến lược phát triển và bảo vệ an ninh mạng 05 năm một lần dựa trên kết quả kiểm tra, đánh giá công tác an ninh mạng, sự phát triển của khoa học công nghệ và nguy cơ an ninh mạng.

6. Các bộ, ngành, cơ quan nhà nước định kỳ tổng kết công tác bảo vệ an ninh mạng, xây dựng kế hoạch bảo vệ an ninh mạng, xác định rõ các mục tiêu ngắn hạn, trung hạn, dài hạn.

7. Bộ Công an chủ trì, phối hợp với Bộ Giáo dục và Đào tạo đánh giá, phổ biến, phát triển và đưa các khái niệm và thực tiễn an ninh mạng vào chương trình giảng dạy chính của các chương trình khoa học máy tính và chương trình khác để xây dựng chuyên ngành giáo dục an ninh mạng trong hệ thống các trường đại học, cao đẳng.

### Điều 39. An ninh thông tin mạng

1. Nhà nước xây dựng môi trường không gian mạng lành mạnh, hệ thống pháp luật về an ninh mạng được hoàn thiện, tôn trọng và thực thi nghiêm túc, người dân ứng xử có quy tắc trên không gian mạng, tham gia không gian mạng an toàn và được bảo vệ, xử lý nghiêm mọi hành vi vi phạm quy định của pháp luật.

2. Huy động sức mạnh của hệ thống chính trị và toàn dân trong đấu tranh phản bác, vô hiệu hóa các thông tin chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, 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.

3. Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân phải đăng tải thông tin phù hợp với quy định của pháp luật, không cung cấp, đăng tải, truyền đưa những thông tin có nội dung không phù hợp với lợi ích đất nước.

4. Các doanh nghiệp dịch vụ viễn thông, internet phải thiết lập cơ chế xác thực thông tin khi người dùng đăng ký tài khoản số để bảo đảm tính bảo mật và tính trung thực của thông tin đăng ký. Người đăng ký tài khoản số có trách nhiệm bảo vệ và sử dụng các tài khoản do mình tạo lập đúng quy định của pháp luật.

5. Các doanh nghiệp nước ngoài khi cung cấp dịch vụ viễn thông, internet tại Việt Nam phải tuân thủ pháp luật, tôn trọng chủ quyền, lợi ích và an ninh quốc gia Việt Nam và lợi ích của người sử dụng, có giấy phép hoạt động, đặt cơ quan đại diện và máy chủ quản lý dữ liệu người sử dụng Việt Nam trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam; bảo mật thông tin người dùng và thông tin tài khoản của người dùng; xử lý nghiêm các hành vi sai phạm theo quy định của pháp luật.

6. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan xây dựng, trình Chính phủ ban hành Bộ Quy tắc ứng xử trên không gian mạng, khuyến khích hành vi chuẩn mực, phù hợp với đạo đức, thuần phong mỹ tục trên không gian mạng.

### Điều 40. Giáo dục và nâng cao nhận thức về an ninh mạng

1. Nhà 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:

a) Tăng cường nhận thức của cơ quan nhà nước, tổ chức, công dân về an ninh mạng;

b) Phổ biến rộng rãi các tiêu chuẩn kỹ thuật và thực tiễn an ninh mạng;

c) Áp dụng những biện pháp bảo vệ an ninh mạng phù hợp;

d) Đào tạo nguồn nhân lực an ninh mạng chất lượng cao;

đ) Thúc đẩy các sáng kiến về đánh giá, dự báo an ninh mạng.

2. Bộ Công an phối hợp với các bộ, ngành liên quan xây dựng, triển khai kế hoạch giáo dục và nâng cao nhận thức về an ninh mạng.

### Điều 41. Bảo đảm an ninh mạng trong ứng dụng, quản lý, vận hành điện toán đám mây

1. Nghiên cứu, triển khai ứng dụng, vận hành, quản lý điện toán đám mây an toàn, bảo mật trong cơ quan hành chính nhà nước và tổ chức, cá nhân.

2. Thúc đẩy sự phát triển của điện toán đám mây thông qua sự phối hợp với khu vực tư nhân để tiêu chuẩn hóa điện toán đám mây trong cơ quan hành chính nhà nước.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành và tổ chức liên quan:

a) Bảo đảm an ninh vật lý của trung tâm dữ liệu điện toán đám mây và các dữ liệu được lưu giữ trong trung tâm dữ liệu điện toán đám mây;

b) Bảo đảm sự tiếp cận an toàn đối với các dữ liệu được lưu trữ trong trung tâm điện toán đám mây;

c) Phát triển các tiêu chuẩn bảo mật điện toán đám mây;

d) Hỗ trợ phát triển quá trình tự động hóa các hệ thống giám sát liên tục bảo đảm an ninh mạng đối với trung tâm dữ liệu điện toán đám mây.

### Điều 42. Bảo đảm an ninh mạng đối với hệ thống liên kết thế giới thực và ảo

1. Nhà nước xác định bảo đảm an ninh mạng đối với hệ thống liên kết thế giới thực và ảo là nhiệm vụ trọng tâm trong chiến lược nghiên cứu phát triển và bảo vệ an ninh mạng.

2. Xây dựng phương án bảo đảm an ninh mạng đối với các hệ thống liên kết thế giới thực và ảo trước xu thế ứng dụng công nghệ thông tin, tự động hóa, hội nhập quốc tế ngày càng sâu rộng.

3. Đánh giá, dự báo khả năng phát triển và ảnh hưởng xã hội của các hệ thống liên kết thế giới thực và ảo.

### Điều 43. Bảo đảm an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng internet quốc tế

1. Chính phủ ban hành quy định quản lý bảo đảm an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng internet quốc tế, xác lập quyền quản lý, kiểm soát hoạt động kết nối mạng internet quốc tế.

2. Quản lý nhà nước về an ninh mạng đối với hoạt động cung cấp dịch vụ viễn thông, internet và thông tin qua biên giới.

3. Bộ Công an triển khai các biện pháp bảo đảm an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng internet quốc tế.

### Điều 44. Nghiên cứu và phát triển quản lý định danh

1. Thực thi chính sách xác thực tài khoản số, nghiên cứu phát triển kỹ thuật xác thực tài khoản số an toàn và thuận tiện.

2. Nghiên cứu, xây dựng các tiêu chuẩn kỹ thuật đối với các công nghệ, hệ thống quản lý định danh nhằm:

a) Tăng cường khả năng tương tác giữa công nghệ quản lý định danh;

b) Tăng cường các phương pháp xác thực của hệ thống quản lý định danh;

c) Tăng cường bảo vệ quyền riêng tư trong các hệ thống quản lý định danh, bao gồm các hệ thống thông tin liên quan tới sức khỏe;

d) Phát triển các giao thức bảo mật và xác thực;

đ) Tăng cường khả năng sử dụng các hệ thống quản lý định danh.

3. Bộ Công an chủ trì, phối hợp với Ban Cơ yếu Chính phủ, Bộ Thông tin và Truyền thông, Bộ Khoa học và Công nghệ trong nghiên cứu và phát triển quản lý định danh.

### Điều 45. Bảo vệ an ninh mạng theo cấp độ

1. Nhà nước thực hiện chế độ bảo vệ an ninh mạng theo cấp độ.

2. Tiêu chí phân định cấp độ bảo vệ an ninh mạng:

a) Tính chất quan trọng của thông tin và hệ thống thông tin;

b) Phạm vi ảnh hưởng;

c) Khả năng gây thiệt hại của hành vi vi phạm pháp luật trên không gian mạng.

3. Doanh nghiệp cung cấp dịch vụ viễn thông, internet phải căn cứ vào yêu cầu của cấp độ bảo vệ an ninh mạng để thực hiện nghĩa vụ an ninh mạng sau đây nhằm bảo vệ mạng khỏi sự can thiệp, phá hoại hoặc truy cập trái phép, ngăn chặn rò rỉ, lộ lọt, chiếm đoạt, giả mạo dữ liệu mạng:

a) Xây dựng chế độ quản lý, quy trình thao tác bảo đảm an ninh mạng trong nội bộ, xác định người phụ trách về an ninh mạng;

b) Áp dụng biện pháp kỹ thuật ngăn chặn các đe dọa an ninh mạng như: virut máy tính, tấn công mạng, xâm nhập mạng;

c) Áp dụng biện pháp kỹ thuật kiểm tra, giám sát, ghi lại hoạt động mạng và sự cố an ninh mạng, lưu giữ bản ghi ít nhất 12 tháng;

d) Áp dụng các biện pháp phân loại dữ liệu, sao lưu và mã hóa dữ liệu quan trọng;

đ) Các nghĩa vụ khác theo pháp luật.

4. Chính phủ quy định chi tiết về cấp độ bảo vệ an ninh mạng.

5. Bộ Công an chủ trì, phối hợp với Bộ Thông tin và Truyền thông kiểm tra, giám sát nghĩa vụ bảo vệ an ninh mạng theo cấp độ của cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia và các doanh nghiệp cung cấp dịch vụ viễn thông, internet.

### Điều 46. Kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin thuộc cơ quan, tổ chức, doanh nghiệp nhà nước

1. Chính phủ kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống mạng thông tin thuộc cơ quan, tổ chức, doanh nghiệp nhà nước.

2. Việc kiểm tra, đánh giá thực trạng an ninh mạng là trách nhiệm của cơ quan chủ quản hệ thống thông tin. Cơ quan chuyên trách bảo vệ an ninh mạng tổ chức kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống mạng thông tin của các cơ quan, tổ chức, doanh nghiệp nhà nước khi thấy cần thiết.

3. Cơ quan chuyên trách kiểm tra, đánh giá thực trạng an ninh mạng

a) Bộ Công an kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của các bộ, ban, ngành chức năng và UBND cấp tỉnh, thành phố trực thuộc Trung ương; phối hợp với Ban Cơ yếu Chính phủ kiểm tra, đánh giá thực trạng an ninh mạng với hệ thống mạng liên lạc cơ yếu do Ban Cơ yếu Chính phủ quản lý;

b) Bộ Quốc phòng kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin quân sự do Bộ Quốc phòng quản lý;

c) Bộ Thông tin và Truyền thông kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thông thông tin thuộc khối cơ quan, tổ chức, doanh nghiệp nhà nước không thuộc quy định tại Điểm a, Điểm b, Khoản 2 Điều này.

4. Thời điểm kiểm tra, đánh giá thực trạng an ninh mạng

a) Trước khi hệ thống thông tin được đưa vào vận hành, sử dụng;

b) Trong quá trình vận hành, khai thác hệ thống thông tin.

c) Khi có yêu cầu quản lý nhà nước về an ninh mạng.

5. Nội dung kiểm tra, đánh giá thực trạng an ninh mạng

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

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

c) Phương án ứng cứu, khắc phục sự cố của cơ quan chủ quản hệ thống thông tin.

d) Các tiêu chuẩn bảo mật thông tin tránh rò rỉ qua các kênh kỹ thuật;

đ) Đội ngũ nhân lực bảo vệ an ninh mạng.

6. Quy trình kiểm tra, đánh giá thực trạng an ninh mạng:

a) Cơ quan chủ quản hệ thống thông tin tự tổ chức kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin do mình quản lý tối thiểu một năm một lần và định kỳ gửi báo cáo về cơ quan chuyên trách vào tháng 10 hằng năm.

b) Căn cứ kết quả kiểm tra, đánh giá thực trạng an ninh mạng của cơ quan chủ quản hệ thống thông tin, cơ quan chuyên trách căn cứ vào tiêu chuẩn quốc gia về an ninh mạng để kết luận, lựa chọn cơ quan chủ quản và lập kế hoạch, cử đoàn kiểm tra công tác bảo đảm an ninh mạng.

c) Cơ quan chuyên trách có trách nhiệm công bố danh sách những hệ thống thông tin thuộc diện kiểm tra, đánh giá trên cổng thông tin điện tử của Bộ và có văn bản thông báo trước cho cơ quan chủ quản hệ thống thông tin trước 01 tháng.

d) Cơ quan chuyên trách có quyền kiểm tra đột xuất đối với các trường hợp sau đây:

- Hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật và các hành vi vi phạm quy định về công tác bảo vệ an ninh mạng theo khuyến cáo của cơ quan chuyên trách đưa ra dựa trên kết quả kiểm tra gần nhất mà những điểm yếu, lỗ hổng bảo mật và các hành vi vi phạm quy định về công tác bảo vệ an ninh mạng này có khả năng gây ra sự cố ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia và trật tự an toàn xã hội;

- Xảy ra sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia;

- Quyết định của Thủ tướng Chính phủ hoặc Thủ trưởng cơ quan chuyên trách về việc kiểm tra đột xuất hệ thống hạ tầng thông tin.

đ) Sau khi tiến hành kiểm tra các hệ thống thông tin, cơ quan chuyên trách đưa ra kết luận về tình trạng bảo vệ an ninh mạng của hệ thống và khuyến cáo để cải thiện tình trạng bảo mật an ninh mạng cho hệ thống đó. Kết quả gửi về cho cơ quan chủ quản hệ thống thông tin trong thời hạn 30 ngày kể từ khi kết thúc hoạt động kiểm tra.

7. Kết quả kiểm tra, đánh giá thực trạng an ninh mạng:

a) Là căn cứ để cơ quan chủ quản hệ thống thông tin tổ chức công tác khắc phục tồn tại, hạn chế.

b) Là căn cứ để cấp chứng nhận hợp chuẩn về an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

8. Công tác kiểm tra, đánh giá bảo vệ an ninh mạng đối với hệ thống thông tin được tiến hành định kỳ hằng năm, tối thiểu ba năm một lần, tối đa không quá năm năm một lần kể từ khi cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia khai báo, đăng ký hoạt động của hệ thống thông tin hoặc lần kiểm tra, đánh giá hệ thống thông tin quan trọng về an ninh quốc gia gần nhất, ngoại trừ các quy định tại điểm d, Khoản 4 Điều này.

### Điều 47. Nâng cao năng lực tự chủ về an ninh mạng

1. Nhà nước khuyến khích và tạo mọi điều kiện để xây dựng nền công nghiệp an ninh mạng có khả năng sản xuất, kiểm tra, đánh giá và kiểm định sản phẩm, dịch vụ mạng, đưa lĩnh vực an ninh mạng trở thành một ngành “công nghiệp tăng trưởng” có khả năng tạo các cơ hội việc làm.

2. Chính phủ triển khai các biện pháp cần thiết về an ninh mạng để nâng cao năng lực tự chủ về an ninh mạng bao gồm: thúc đẩy nghiên cứu, phát triển các sản phẩm, dịch vụ an ninh mạng; thúc đẩy các tiến bộ công nghệ liên quan an ninh mạng; đào tạo, phát triển và tuyển dụng nhân lực an ninh mạng; 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; tham gia các khuôn khổ quốc tế về an ninh mạng trên cơ sở công nhận lẫn nhau.

### Điều 48. Hợp tác quốc tế về an ninh mạng

1. Tổ chức, cá nhân Việt Nam hợp tác về an ninh mạng với tổ chức, cá nhân nước ngoài, tổ chức quốc tế 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

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

b) Cơ chế, chính sách 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 đảm 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) Đào tạo, phát triển nguồn nhân lực an ninh mạng;

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

g) Ký kết, gia nhập và thực hiện điều ước quốc tế song phương, đa phương và tham gia tổ chức khu vực, tổ chức quốc tế về an ninh mạng;

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

# *Chương IV*

# ĐÀO TẠO, PHÁT TRIỂN NGUỒN NHÂN LỰC AN NINH MẠNG

### Điều 49. Chính sách đào tạo, phát triển nguồn nhân lực an ninh mạng

1. Nhà nước ưu tiên đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao, có phẩm chất đạo đức tốt, đáp ứng yêu cầu xây dựng và bảo vệ Tổ quốc.

2. Việc đào tạo, phát triển nguồn nhân lực an ninh mạng được thực hiện tại các cơ sở đào tạo, tổ chức giáo dục trong và ngoài nước.

3. Bộ Công an chủ trì, phối hợp với Bộ Giáo dục và Đào tạo xây dựng chương trình, biện pháp để phát hiện, tuyển chọn nguồn nhân lực chất lượng cao cho công tác an ninh mạng.

### Điều 50. Phát triển nguồn nhân lực an ninh mạng

1. Nội dung đào tạo về an ninh mạng là một bộ phận trong chương trình giáo dục đào tạo đại học, cao đẳng và tương đương.

2. Người làm công tác an ninh mạng trong cơ quan nhà nước được hưởng chế độ đãi ngộ phù hợp.

3. Bộ Giáo dục và Đào tạo quy định cụ thể về việc mở ngành đào tạo về an ninh mạng.

4. Bộ Nội vụ chủ trì, phối hợp với các cơ quan liên quan tổ chức bồi dưỡng kiến thức an ninh mạng cho cán bộ, công chức, viên chức.

5. Bộ Công an chủ trì, phối hợp với các bộ, ngành có liên quan tổ chức bồi dưỡng chuyên gia an ninh mạng phục vụ công tác bảo vệ chủ quyền, lợi ích, an ninh quốc gia, bảo đảm trật tự an toàn xã hội.

### Điều 51. Văn bằng, chứng chỉ về an ninh mạng

1. Cơ sở đào tạo trong phạm vi, nhiệm vụ, quyền hạn của mình cấp văn bằng, chứng chỉ đào tạo về an ninh mạng.

2. Bộ Giáo dục và Đào tạo chủ trì, phối hợp với Bộ Công an công nhận văn bằng, chứng chỉ giáo dục đại học về an ninh mạng do tổ chức nước ngoài cấp.

3. Bộ Lao động, Thương binh và Xã hội chủ trì, phối hợp với Bộ Công an công nhận văn bằng, chứng chỉ giáo dục nghề nghiệp về an ninh mạng do tổ chức nước ngoài cấp.

### Điều 52. Phổ biến kiến thức an ninh mạng

1. Nhà nước có chính sách khuyến khích phổ biến kiến thức an ninh mạng trong phạm vi cả nước.

2. 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 an ninh mạng cho tổ chức, cá nhân trong địa phương mình.

3. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Bộ Giáo dục và Đào tạo đưa kiến thức an ninh mạng vào chương trình giáo dục quốc phòng, an ninh.

4. Nhà nước có chính sách hỗ trợ việc học tập, phổ biến kiến thức về an ninh mạng đối với người tàn tật, người nghèo, người dân tộc thiểu số và các đối tượng ưu tiên khác phù hợp với yêu cầu phát triển trong từng thời kỳ theo quy định của Chính phủ.

5. Cơ quan chuyên trách bảo vệ an ninh mạng có trách nhiệm tổ chức phổ biến kiến thức an ninh mạng hằng năm theo chức năng, nhiệm vụ được giao.

# *Chương V*

# TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

### Điều 53. Quyền và trách nhiệm của tổ chức, cá nhân tham gia sử dụng không gian mạng

1. Tổ chức, cá nhân tham gia sử dụng không gian mạng được yêu cầu doanh nghiệp cung cấp dịch vụ viễn thông, internet sửa, xóa hoặc đính chính thông tin liên quan tới bản thân mình trên hệ thống, dịch vụ của các doanh nghiệp cung cấp dịch vụ viễn thông, internet nếu có căn cứ cho rằng, thông tin đó không đúng hoặc được thu thập, sử dụng trái quy định pháp luật và cam kết giữa hai bên.

2.Chịu trách nhiệm với hoạt động trên không gian mạng của mình.

3.Không sử dụng công nghệ, kỹ thuật, tạo ra mã độc nhằm mục đích thực hiện hành vi vi phạm pháp luật; không bán hoặc cung cấp thông tin cá nhân trái pháp luật hoặc chưa được sự đồng ý của người sở hữu thông tin.

4.Không cài đặt các chương trình độc hại hay có chứa các nội dung bị cấm đăng, tán phát theo quy định của pháp luật khi đăng tải các thông tin điện tử, cung cấp phần mềm, ứng dụng.

5. Đấu tranh với các hành vi xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng.

### Điều 54. Trách nhiệm của chủ thể sản xuất, kinh doanh sản phẩm, dịch vụ mạng

1. Tuân thủ các điều kiện bảo đảm chất lượng đối với sản phẩm trước khi đưa ra thị trường theo quy định của pháp luật và chịu trách nhiệm về chất lượng sản phẩm do mình sản xuất.

2. Thể hiện thông tin về chất lượng, thành phần sản phẩm, dịch vụ mạng theo quy định của pháp luật.

3. Thông tin trung thực về chất lượng sản phẩm, dịch vụ mạng.

4. Cảnh báo về khả năng gây mất an ninh mạng của sản phẩm, dịch vụ mạng và cách phòng ngừa.

5. Cung cấp thông tin về việc bảo hành và thực hiện bảo hành sản phẩm, dịch vụ mạng.

6. Kịp thời ngừng sản xuất, thông báo cho các bên liên quan và các biện pháp khắc phục hậu quả khi phát hiện sản phẩm, dịch vụ mạng gây mất an ninh mạng hoặc không phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật áp dụng tương ứng.

7. Thu hồi, xử lý sản phẩm, dịch vụ mạng không bảo đảm chất lượng.

8. Tuân thủ các quy định về thanh tra, kiểm tra của cơ quan nhà nước có thẩm quyền.

### Điều 55. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, internet

1. Trong triển khai công tác bảo vệ an ninh mạng

a) Yêu cầu người dùng cung cấp thông tin cá nhân xác thực. Nếu người dùng không cung cấp thông tin cá nhân thực, nhà cung cấp dịch vụ có trách nhiệm từ chối cung cấp các dịch vụ liên quan cho người dùng đó.

b) 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 cơ quan chủ quản theo quy định.

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

d) Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm đảm bảo 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 tới cơ quan chủ quản theo quy định.

2. Trong bảo đảm an ninh thông tin mạng

a) Bảo mật thông tin cá nhân người dùng theo quy định của pháp luật, đồng thời xây dựng, kiện toàn chính sách bảo vệ thông tin cá nhân.

b)Nghiêm cấm tiết lộ, thay đổi, gây tổn hại đến thông tin cá nhân người dùng; khi chưa được sự cho phép của người sở hữu thông tin, không được cung cấp thông tin cho bên thứ ba.

c) Sửa, xóa hoặc đính chính thông tin thu thập trái pháp luật theo yêu cầu người dùng;

d)Ngăn chặn việc chia sẻ thông tin, tiến hành xóa thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, thông tin sai sự thật, vu khống trên không gian mạng, đồng thời lưu lại các ghi chép liên quan để báo cáo với cơ quan chuyên trách;

đ) Không cung cấp dịch vụ viễn thông, internet, hỗ trợ kỹ thuật, quảng cáo, hỗ trợ thanh toán cho các tổ chức, cá nhân đăng tải thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, thông tin sai sự thật, vu khống trên không gian mạng.

e) Xây dựng, kiện toàn quy trình bảo vệ và cơ chế hợp tác an ninh mạng, tăng cường đánh giá, phân tích các loại rủi ro an ninh mạng, định kỳ cảnh báo nguy cơ, đồng thời ủng hộ, giúp đỡ các thành viên nâng cao khả năng ứng phó với rủi ro an ninh mạng.

g) Xây dựng cơ chế phản hồi, khiếu nại về an ninh thông tin mạng; công bố thông tin về phương thức phản hồi, khiếu nại; kịp thời tiếp nhận và xử lý các phản hồi, khiếu nại liên quan an ninh thông tin mạng.

h) Loại bỏ 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 trong vòng 24 giờ sau khi nhận được phản hồi, khiếu nại từ người dùng; lưu lại bản ghi trong vòng 12 tháng.

i) Thực hiện yêu cầu của cơ quan chức năng Bộ Công an, Bộ Thông tin và Truyền thông trong ngăn chặn, xử lý thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, thông tin sai sự thật, vu khống trên không gian mạng.

### Điều 56. Trách nhiệm của cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia

1. Thành lập bộ phận chuyên trách hoặc phân công cá nhân phụ trách bảo đảm an ninh mạng.

2. Xây dựng quy chế vận hành, bảo đảm an ninh mạng, xác định cấp độ cần 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 cứu, khắc phục sự cố khi có sự cố an ninh mạng hoặc thảm họa xảy ra.

3. Bảo đảm hệ thống thông tin quan trọng về an ninh quốc gia đáp ứng tiêu chuẩn quốc gia về an ninh mạng, quy chuẩn kỹ thuật về an ninh mạng.

4. Khi thu thập, tạo ra thông tin cá nhân và dữ liệu quan trọng phải lưu trữ trong phạm vi quốc gia. Nếu bắt buộc phải cung cấp thông tin ra bên ngoài phạm vi quốc gia, phải đánh giá mức độ an ninh theo quy định của Bộ Công an, trong trường hợp có luật quy định thì căn cứ theo nội dung của luật đó để tiến hành.

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 đảm an ninh mạng trước khi thiết lập, mở rộng, nâng cấp hệ thống thông tin quan trọng về an ninh quốc gia.

6. Tiến hành hoặc ủy thác cho tổ chức cung cấp dịch vụ an ninh mạng tiến hành khảo sát, đánh giá mức độ an toàn và khả năng ứng phó rủi ro của cơ sở đó ít nhất 02 lần/năm, đồng thời gửi báo cáo tình hình kiểm tra, đánh giá, cải tiến biện pháp khắc phục tới cơ quan chuyên trách thuộc Bộ Công an.

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

### Điều 57. Trách nhiệm của Bộ Công an

1. Bộ Công an giúp Chính phủ quản lý nhà nước về an ninh mạng trên phạm vi toàn quốc.

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

3. 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.

4. 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.

5. Bảo đảm an ninh thông tin mạng; 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.

6. Bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

7. Thực hiện quản lý nhà nước trong bảo đảm an ninh mạng đối với các sản phẩm, dịch vụ mạng; kiểm tra, đánh giá, thẩm định hoặc chỉ định tổ chức kiểm tra, đánh giá, thẩm định sự phù hợp về an ninh mạng đối với các sản phẩm, dịch vụ mạng trước khi đưa vào sử dụng trong các hệ thống thông tin quan trọng về an ninh quốc gia, cơ quan chứa đựng bí mật nhà nước, công trình trọng yếu quốc gia.

8. Cấp Giấy phép kinh doanh dịch vụ bảo đảm an ninh mạng cho các tổ chức, cá nhân.

9. Bảo vệ bí mật nhà nước trên không gian mạng.

10. Tổ chức kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin của cơ quan nhà nước, hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của các công trình trọng yếu quốc gia, mục tiêu quan trọng về an ninh quốc gia, cơ quan chứa đựng bí mật nhà nước.

11. Quản lý 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 đảm an ninh mạng của các doanh nghiệp cung cấp dịch vụ viễn thông, internet.

12. 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.

13. Điều phối, ứng cứu, khắc phục sự cố an ninh mạng.

14. Phối hợp với Bộ Khoa học và Công nghệ xây dựng, công bố tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng; đăng ký, chỉ định và quản lý hoạt động của tổ chức đánh giá chứng nhận hợp chuẩn, hợp quy về an ninh mạng.

15. Phối hợp với Bộ Giáo dục và Đào tạo trong đào tạo, phát triển nguồn nhân lực an ninh mạng.

16. Phân công lực lượng an ninh mạng chuyên trách trực thuộc và tại Công an các tỉnh, thành phố trực thuộc Trung ương.

17. Xử lý các hành vi vi phạm pháp luật về an ninh mạng;

18. Hợp tác quốc tế về an ninh mạng.

### Điều 58. Trách nhiệm của Bộ Quốc phòng

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

2. 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 tác chiến không gian mạng.

3. Chủ trì, phối hợp với các bộ, ngành liên quan trong phòng, chống chiến tranh mạng theo chức năng, nhiệm vụ được giao.

4. Thẩm định về an ninh mạng trong hồ sơ thiết kế, xây dựng, đầu tư mua sắm thiết bị cho hệ thống thông tin quân sự;

5. Kiểm tra, đánh giá thực trạng an ninh mạng, ứng cứu, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quân sự;

6. Thực hiện công tác giám sát an ninh thông tin mạng đối với hệ thống thông tin của Bộ Quốc phòng;

7. Bảo vệ bí mật quân sự, bí mật nhà nước trên không gian mạng 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.

8. Phối hợp với Bộ Công an 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.

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

### Điều 59. Trách nhiệm của Bộ Thông tin và Truyền thông

1. Trong quản lý nhà nước về an toàn thông tin mạng:

a) 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 toàn thông tin mạng;

b) Kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin của tổ chức, cá nhân là doanh nghiệp có hệ thống thông tin không nằm trong hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quân sự;

c) Phối hợp với Bộ Công an trong triển khai thực hiện công tác bảo vệ an ninh mạng theo chức năng, nhiệm vụ được giao;

d) Thực hiện hợp tác quốc tế về an toàn thông tin mạng.

2. Trong ngăn chặn, xử lý thông tin có nội dung chống Nhà nước trên không gian mạng:

a) Chủ động phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước trên không gian mạng, huy động quần chúng nhân dân tham gia phản bác thông tin xấu, độc hại trên không gian mạng;

b) Chỉ đạo các nhà cung cấp dịch vụ viễn thông, internet, cơ quan chủ quản trang thông tin điện tử, cổng thông tin điện tử loại bỏ thông tin có nội dung chống Nhà nước trên không gian mạng, xử lý nghiêm các trường hợp vi phạm;

c) Chỉ đạo cơ quan thông tấn, báo chí tăng cường tuyên truyền, định hướng dư luận, nghiêm cấm báo chí đăng lại thông tin chưa được kiểm chứng từ internet;

d) Yêu cầu các nhà cung cấp dịch vụ viễn thông, internet nước ngoài chấp hành nghiêm pháp luật Việt Nam, đăng ký kinh doanh và đặt máy chủ chứa dữ liệu người dùng Việt Nam trên lãnh thổ Việt Nam.

### Điều 60. Trách nhiệm của các bộ, ngành liên quan

1. Bộ Khoa học và Công nghệ

a) Xác định và tổ chức thực hiện các nhiệm vụ khoa học và công nghệ liên quan đến công tác an ninh mạng;

b) Chủ trì, phối hợp với cơ quan có liên quan phê duyệt quy hoạch, kế hoạch xây dựng tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng, tổ chức thẩm định và công bố tiêu chuẩn quốc gia về an ninh mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

2. Bộ Nội vụ

a)Phối hợp với Bộ Công an xây dựng chính sách, cơ chế phối hợp thu hút, trọng dụng, đãi ngộ nguồn nhân lực chất lượng cao về công nghệ thông tin, chuyên gia an ninh mạng;

b) Phối hợp với Bộ Công an tổ chức hướng dẫn bồi dưỡng kiến thức an ninh mạng cho cán bộ, công chức, viên chức; bổ sung tiêu chuẩn kiến thức về an ninh mạng đối với chức danh lãnh đạo trong bộ máy cơ quan nhà nước;

c) Bảo đảm chế độ, chính sách cho lực lượng an ninh mạng.

3. Bộ Giáo dục và Đào tạo

a) Chủ trì, phối hợp với Bộ Công an trong đào tạo, phát triển nguồn nhân lực an ninh mạng; quy định cụ thể về việc mở ngành đào tạo về an ninh mạng.

b) Phối hợp với Bộ Công an đào tạo nguồn nhân lực an ninh mạng chất lượng cao, có phẩm chất đạo đức tốt; công nhận văn bằng, chứng chỉ giáo dục đại học về an ninh mạng do tổ chức nước ngoài cấp;

c) Phối hợp với Bộ Công an, Bộ Quốc phòng xây dựng chương trình và đưa kiến thức an ninh mạng vào chương trình giáo dục quốc phòng, an ninh.

4. Bộ Lao động, Thương binh và Xã hội có trách nhiệm tổ chức đào tạo, bồi dưỡng, phổ biến kiến thức về an ninh mạng trong cơ sở giáo dục nghề nghiệp.

5. Bộ Tài chính

a) Hướng dẫn, bảo đảm kinh phí duy trì hoạt động bảo vệ an ninh mạng;

b) Bảo đảm chế độ, chính sách cho lực lượng an ninh mạng.

6. Bộ Kế hoạch và Đầu tư

a) Hướng dẫn và đầu tư trang thiết bị cho hoạt động bảo vệ an ninh mạng;

b) Phối hợp với Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông trong triển khai các dự án, đề án, chương trình, kế hoạch đầu tư cho hoạt động bảo vệ an ninh mạng.

7. Bộ Ngoại giao

a) Phối hợp với Bộ Công an trong quảng bá, tuyên truyền chính sách an ninh mạng của Việt Nam;

b) Nghiên cứu, phối hợp với Bộ Công an trong tham gia các điều ước, thỏa thuận quốc tế về an ninh mạng.

8. Bộ Công thương:

a) Phối hợp với Bộ Công an trong quản lý sản phẩm, dịch vụ mạng và cấp phép kinh doanh dịch vụ bảo đảm an ninh mạng.

b) Phối hợp với Bộ Công an bổ sung kinh doanh dịch vụ bảo đảm an ninh mạng vào Phụ lục: Danh mục ngành, nghề kinh doanh có điều kiện theo quy định của pháp luật về đầu tư.

9. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng:

a) Quản lý nhà nước về mật mã quốc gia để bảo mật thông tin thuộc phạm vi bí mật nhà nước trên hệ thống mạng liên lạc cơ yếu.

b) Quản lý nhà nước về mật mã dân sự.

10. Bộ, ngành liên quan trong phạm vi nhiệm vụ, quyền hạn có trách nhiệm thực hiện công tác bảo đảm an ninh mạng của 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.

### Điều 61. Trách nhiệm của ủy ban nhân dân cấp tỉnh

1. Xây dựng, ban hành và hướng dẫn thực hiện quy chuẩn kỹ thuật địa phương về an ninh mạng; quản lý chất lượng sản phẩm, dịch vụ mạng trên địa bàn.

2. Trong phạm vi, nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về an ninh mạng ở địa phương; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng.

### Điều 62. Trách nhiệm của cơ quan chuyên trách bảo vệ an ninh mạng

1. Cơ quan chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thực hiện nhiệm vụ bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng, phòng chống tấn công mạng, gián điệp mạng, khủng bố mạng; bảo đảm an ninh thông tin mạng; an ninh hệ thống mạng thông tin quan trọng về an ninh quốc gia; giám sát, dự báo, ứng cứu và diễn tập ứng cứu sự cố an ninh mạng; triển khai công tác bảo vệ an ninh mạng trên phạm vi toàn quốc.

2. Cơ quan chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng có trách nhiệm thực hiện nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng, phòng chống chiến tranh mạng gắn liền với hoạt động quân sự, chiến tranh thông tin, chiến tranh điện tử do đối phương tiến hành; bảo vệ hệ thống mạng thông tin do Bộ Quốc phòng quản lý.

3. Cơ quan chuyên trách bảo vệ an ninh mạng thuộc Bộ Thông tin và Truyền thông thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng trên phạm vi toàn quốc, phối hợp bảo vệ chủ quyền, an ninh không gian mạng quốc gia.

4. Ban Cơ yếu Chính phủ có trách nhiệm giám sát, bảo vệ hệ thống mạng liên lạc cơ yếu do Ban Cơ yếu Chính phủ quản lý; bảo vệ bí mật nhà nước bằng cơ yếu.

# *Chương VI*

# ĐIỀU KHOẢN THI HÀNH

### Điều 63. Hiệu lực thi hành

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

### Điều 64. Quy định chi tiết

Chính phủ, cơ quan nhà nước có thẩm quyền quy định chi tiết các điều khoản được giao trong Luật.

*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.*

1. Theo Khoản 10 Điều 4 Luật Giao dịch điện tử: “*Phương tiện điện tử là phương tiện hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, điện từ hoặc công nghệ tương tự*”. Như vậy, bao gồm cả hệ thống thông tin, trang thông tin điện tử, cổng thông tin điện tử. [↑](#footnote-ref-2)
2. Tấn công vào một hoặc nhiều hệ thống thông tin quan trọng về an ninh quốc gia theo từng đợt, từng nhóm đối tượng diễn ra trong thời gian ngắn, bất ngờ. [↑](#footnote-ref-3)
3. Hoạt động tấn công vào nhiều hệ thống thông tin quan trọng về an ninh quốc gia trên diện rộng mang tính chất phá hoại, gây cản trở, tê liệt hoạt động thông tin liên lạc, thu thập thông tin tình báo; gây đình trệ, thậm chí phá hỏng sự vận hành bình thường của hệ thống mạng thông tin, hệ thống điều khiển tự động của Việt Nam. [↑](#footnote-ref-4)
4. Thông qua kế hoạch được đối phương tính toán, dự trù từ trước; mang tính chất hủy diệt nhằm vào những mục tiêu trọng yếu, có liên quan tới quốc phòng, an ninh hoặc những mục tiêu dân sự quan trọng có ảnh hưởng tới quốc gia như hệ thống giao thông, điện, nước, ngân hàng, chứng khoán, hệ thống SCADA, cáp quang ngầm dưới biển, hệ thống phòng thủ bờ biển và các hệ thống quân sự khác. [↑](#footnote-ref-5)