BỘ CÔNG AN	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /TTr-BCA	*Hà Nội, ngày tháng năm 2025*

TỜ TRÌNH
Dự án, dự thảo Luật An ninh mạng

Kính gửi: Quốc hội

Thực hiện quy định của Thực hiện quy định của Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 và Nghị định số 78/2025/NĐ-CP, Bộ Công an trình Chính phủ dự án Luật An ninh mạng, cụ thể như sau:

I. SỰ CẦN THIẾT BAN HÀNH LUẬT

1. Cơ sở chính trị, pháp lý

Thời gian vừa qua, trong bối cảnh phát triển vượt bậc của cuộc Cách mạng công nghiệp lần thứ tư, Đảng và Nhà nước ta nhận thức rõ được tầm quan trọng của không gian mạng. Các văn kiện, Nghị quyết của Đảng và Nhà nước ta ban hành gần đây đã đề ra nhiều chủ trương, định hướng quan trọng liên quan đến yêu cầu hoàn thiện thể chế về an ninh mạng, cụ thể như:

- Thực hiện tinh thần Nghị quyết số 18-NQ/TW ngày 25/10/2017 của Bộ Chính trị về một số vấn đề tiếp tục đổi mới, sắp xếp tổ chức bộ máy của hệ thống chính trị tinh gọn, hoạt động hiệu lực, hiệu quả, ngày 18/02/2025, Quốc hội đã ban hành Nghị quyết số 176/2025/QH15 về cơ cấu tổ chức của Chính phủ nhiệm kỳ Quốc hội khóa XV. Theo chủ trương được nêu tại Nghị quyết số 176/2025/QH15 thì nhiệm vụ quản lý nhà nước về bảo đảm an toàn thông tin mạng được chuyển từ Bộ Thông tin và Truyền thông về Bộ Công an.

- Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia đã xác định mục tiêu, nhiệm vụ và giải pháp để bảo vệ an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng, bao gồm: (1) bảo vệ hệ thống thông tin, dữ liệu, tài nguyên số; (2) tăng cường năng lực, nâng cao hiệu quả đấu tranh bảo vệ an ninh mạng; (3) phát triển hạ tầng, công nghệ số; (4) chủ động phòng ngừa, đấu tranh hiệu quả với các hành vi vi phạm pháp luật.

- Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII năm 2021 đã xác định "An ninh mạng ngày càng tác động mạnh, nhiều mặt, đe dọa nghiêm trọng đến sự phát triển ổn định, bền vững của thế giới, khu vực và đất nước ta. Trong thực tiễn thời gian qua cho thấy, không gian mạng đã và đang làm thay đổi phương thức hoạt động, tổ chức cách thức tiến hành chiến tranh, can dự/can thiệp của các nước; cũng như nhiều khía cạnh khác của hoạt động an ninh, quân sự, tình

báo, tội phạm. Tác chiến mạng đã trở thành một loại hình tác chiến hiến đại; an ninh mạng là ưu tiên hàng đầu trong chiến lược an ninh quốc gia của nhiều nước trên thế giới; thậm chí đã được sử dụng là lực lượng, chiến thuật tiên phong, mở đường cho hoạt động quân sự truyền thống; là vũ khí quan trọng để tiến hành âm mưu, ý đồ cách mạng sắc màu, cách mạng đường phố". Qua đó, nhấn mạnh nhiệm vụ "nghiên cứu, chuyển giao, ứng dụng tiến bộ khoa học và công nghệ, đổi mới sáng tạo, nhất là những thành tựu của cuộc Cách mạng công nghiệp lần thứ tư, thực hiện chuyển đổi số quốc gia, phát triển kinh tế số, nâng cao năng suất, chất lượng, hiệu quả...; hoàn thiện hệ thống pháp luật".

- Nghị quyết số 44-NQ/TW ngày 24/11/2023 của Bộ Chính trị về Chiến lược bảo vệ Tổ quốc trong tình hình mới đã nhấn mạnh mục tiêu bảo đảm cao nhất lợi ích quốc gia - dân tộc trên cơ sở bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc; bảo vệ Đảng, Nhà nước, Nhân dân, chế độ xã hội chủ nghĩa; bảo vệ thành quả cách mạng, sự nghiệp đổi mới, công nghiệp hoá, hiện đại hoá; bảo vệ nền văn hoá và uy tín, vị thế quốc tế của đất nước; bảo vệ an ninh quốc gia, an ninh con người, an ninh kinh tế, an ninh mạng; giữ vững an ninh chính trị, trật tự, an toàn xã hội; giữ vững, củng cố, tăng cường môi trường hoà bình để xây dựng, phát triển đất nước; đóng góp tích cực vào gìn giữ hoà bình khu vực, thế giới.

- Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về Đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia đã nhấn mạnh quan điểm "bảo đảm chủ quyền quốc gia trên không gian mạng; bảo đảm an ninh mạng, an ninh dữ liệu, an toàn thông tin của tổ chức và cá nhân là yêu cầu xuyên suốt, không thể tách rời trong quá trình phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia".

- Nghị quyết số 66-NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới đã nhấn mạnh việc tập trung xây dựng pháp luật về khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số, tạo hành lang pháp lý cho những vấn đề mới, phi truyền thống (trí tuệ nhân tạo, chuyên đổi số, chuyển đổi xanh, khai thác nguồn lực dữ liệu, tài sản mã hóa...) để hình thành các động lực tăng trưởng mới, thúc đẩy phát triển lực lượng sản xuất mới, các ngành công nghiệp mới. Xây dựng cơ chế, chính sách đột phá, vượt trội, cạnh tranh cho trung tâm tài chính quốc tế, khu thương mại tự do, khu kinh tế trọng điểm...

- Nghị quyết số 68-NQ/TW ngày 04/5/2025 của Bộ Chính trị về phát triển kinh tế tư nhân tiếp tục đề cập đến vấn đề hoàn thiện khung pháp lý cho các mô hình kinh tế mới, kinh doanh dựa trên công nghệ và nền tảng số, đặc biệt là công nghệ tài chính, trí tuệ nhân tạo, tài sản ảo, tiền ảo, tài sản mã hoá, tiền mã hoá, thương mại điện tử... Có cơ chế thử nghiệm đối với những ngành, lĩnh vực mới trên cơ sở hậu kiểm, phù hợp với thông lệ quốc tế. Hoàn thiện pháp

luật, chính sách về dữ liệu, quản trị dữ liệu, tạo thuận lợi cho doanh nghiệp kết nối, chia sẻ, khai thác dữ liệu, bảo đảm an ninh, an toàn.

2. Cơ sở thực tiễn

Thực tiễn thi hành pháp luật về an ninh mạng ở nước ta thời gian qua cho thấy, công tác bảo đảm an ninh mạng, an toàn thông tin mạng còn tồn tại nhiều vấn đề bất cập. Trong đó nguyên nhân căn bản xuất phát từ sự chồng lấn, mâu thuẫn giữa Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) và Luật An ninh mạng năm 2018. Theo quy định tại Điều 36 Luật An ninh mạng năm 2018: "Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng". Theo quy định tại khoản 2 Điều 52 Luật An toàn thông tin mạng năm 2015: "Bộ Thông tin và Truyền thông chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an toàn thông tin mạng". Ngày 18/02/2025, Quốc hội ban hành Nghị quyết số 176/2025/QH15 về cơ cấu tổ chức của Chính phủ nhiệm kỳ Quốc hội khóa XV, tại Nghị quyết số 176/2025/QH15, Bộ Thông tin và Truyền thông không thuộc cơ cấu tổ chức của Chính phủ nhiệm kỳ Quốc hội khóa XV. Hiện nay, nhiệm vụ quản lý nhà nước về bảo đảm an toàn thông tin mạng được chuyển từ Bộ Thông tin và Truyền thông sang Bộ Công an. Tuy vậy, thực tế đang tồn tại một số vấn đề như:

Thứ nhất, quy định của Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) về quản lý nhà nước về an ninh, an toàn thông tin mạng chưa thống nhất. Sự bất cập trên đã dẫn tới sự thiếu đồng bộ trong các chiến lược bảo mật; có thể gây gián đoạn hoặc ảnh hưởng đến các biện pháp bảo vệ an ninh mạng hoặc tính sẵn sàng của hệ thống thông tin; ảnh hưởng quyền, lợi ích hợp pháp của công dân, cơ quan, tổ chức, doanh nghiệp.

Thứ hai, hiện nay, tại nước ta vẫn chưa có quy định thống nhất về hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quan trọng quốc gia. Theo quy định hiện hành tại Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018), hệ thống thông tin quan trọng quốc gia là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia và phân loại hệ thống thông tin thành 5 cấp độ, trong đó có 03 cấp độ liên quan tới hệ thống thông tin quan trọng về an ninh quốc gia. Luật An ninh mạng năm 2018 quy định hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng. Tuy nhiên, tại Luật An ninh mạng số 2018, hệ thống thông tin được phân loại gồm 02 cấp độ chung còn lại, thuộc đối tượng bảo vệ của an ninh mạng vì là thành phần của cơ sở hạ tầng không gian mạng quốc gia. Nghị định số 53/2022/NĐ-CP của Chính phủ ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng (Điều 3) một lần nữa khẳng định hệ

thống thông tin quan trọng về an ninh quốc gia là hệ thống thống tin của cơ quan nhà nước và tổ chức chính trị của nước Cộng hòa xã hội chủ nghĩa Việt Nam. Những hệ thống này khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ tác động, gây hậu quả, thiệt hại nghiêm trọng đến an ninh thông tin, an ninh quốc gia, ảnh hưởng trực tiếp đến hoạt động, sự an toàn, ổn định, phát triển của hệ thống thông tin và chính trị, kinh tế - xã hội của đất nước. Trong khi đó, danh mục hệ thống thông tin quan trọng về an ninh quốc gia chưa được ban hành để triển khai thực hiện và tập trung nguồn lực bảo vệ.

Thứ ba, chưa có quy định thống nhất về lực lượng chuyên trách bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia và quy định lực lượng chuyên trách bảo vệ an ninh mạng tại các địa phương. Mặc dù tại các văn bản quy phạm pháp luật hiện hành đã có quy định về trách nhiệm của tổ chức, cá nhân trong bảo vệ an ninh mạng, bảo vệ an toàn thông tin nhưng chưa có quy định một lực lượng chuyên trách và thống nhất để bảo vệ an ninh mạng. Điều này dẫn đến sự chồng chéo trong các nhiệm vụ và thiếu tính đồng bộ trong việc triển khai các biện pháp bảo vệ an ninh mạng.

Thứ tư, quy định về trách nhiệm của người sử dụng mạng và hành vi vi phạm pháp luật về an ninh mạng còn tồn tại nhiều mâu thuẫn. Luật An ninh mạng 2018 yêu cầu cá nhân và tổ chức phải chịu trách nhiệm về các hành vi vi phạm liên quan đến an ninh mạng, ví dụ như phát tán thông tin sai lệch, tấn công mạng, hay xâm phạm quyền lợi của quốc gia. Tuy nhiên, các quy định lại mâu thuẫn với Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018). Bởi Luật An toàn thông tin mạng năm 2015 nhấn mạnh tầm quan trọng của bảo vệ quyền riêng tư và dữ liệu cá nhân. Việc triển khai các biện pháp giám sát quá mức có thể xâm phạm quyền tự do cá nhân và gây mâu thuẫn với các nguyên tắc bảo vệ thông tin cá nhân, đặc biệt là trong môi trường công nghệ số hiện nay, nơi mà các quyền riêng tư được xem là một trong những yếu tố quan trọng đối với người dùng internet.

Nguyên nhân phát sinh vấn đề trên cơ bản đến từ việc thiếu nhận thức đồng nhất trong việc xác định và phân định các khái niệm liên quan đến an ninh mạng và an toàn thông tin mạng, kéo theo đó là trách nhiệm pháp lý của các bộ ngành. Do đó, việc hợp nhất hai văn bản pháp luật trên trong thời điểm này là yêu cầu mang tính thời đại để theo kịp với những tiến bộ khoa học - kỹ thuật, bao trùm những công nghệ mới và có khả năng thích nghi tốt với những xu hướng mới của các hành vi trên không gian mạng. Qua tổng kết, đánh giá công tác bảo đảm an ninh mạng xuyên suốt thời gian hiệu lực của Luật An ninh mạng năm 2018, Bộ Công an đã có một số nhận định như sau:

Thứ nhất, hoạt động tấn công mạng, gián điệp mạng và lộ, mất bí mật nhà nước tại Việt Nam diễn ra ngày càng phức tạp, ảnh hưởng nghiêm trọng đến

an ninh quốc gia. Tin tặc sử dụng nhiều thủ đoạn tinh vi, không ngừng nâng cấp, cải tiến các dòng mã độc để tiến hành các chiến dịch tấn công mạng nhằm vào các cơ quan, tổ chức, doanh nghiệp của Việt Nam. Mục tiêu chủ yếu nhằm vào hệ thống mạng thông tin của các cơ quan Trung ương và các tập đoàn, doanh nghiệp quan trọng. Mục tiêu tấn công không chỉ nhằm thu thập thông tin tình báo, bí mật nhà nước, đặc biệt là các chủ trương, chính sách đối ngoại, an ninh, quốc phòng của Việt Nam mà còn chuẩn bị sẵn để tiến hành các hành động tình báo, phát động các cuộc tấn công phá hoại khi cần thiết. Hàng năm, Bộ Công an phát hiện trên 2.600 trang/cổng thông tin điện tử của Việt Nam (có tên miền ".vn") bị tin tặc tấn công, thay đổi giao diện hoặc chèn tập tin; hàng chục vụ lộ tài liệu bí mật nhà nước với hàng trăm đầu tài liệu; hàng trăm TB dữ liệu của các bộ, ban, ngành, địa phương bị tin tặc chiếm đoạt, trong đó có nhiều tài liệu bí mật nhà nước. Một số cơ quan, đơn vị mặc dù đã được kiểm tra, cảnh báo về các nguy cơ gây mất an ninh mạng, lộ mất bí mật nhà nước, nhưng vẫn để xảy ra tình trạng tiếp diễn.

Thứ hai, việc kiểm soát, quản trị và bảo vệ dữ liệu chưa tương xứng với giá trị và mức độ khai thác, sử dụng dữ liệu trong nền kinh tế số, xã hội số. Dữ liệu cá nhân đang được khai thác, sử dụng, tạo ra giá trị thặng dư một cách tự do, thiếu nguyên tắc và sự quản lý, dẫn tới thực trạng lộ, lọt, mua bán, xâm phạm dữ liệu cá nhân diễn ra phổ biến, ngày càng nghiêm trọng, kéo theo gia tăng các loại tội phạm mạng, tội phạm lừa đảo chiếm đoạt tài sản.

Thứ ba, hoạt động phá hoại tư tưởng, chống đối trong nước nhằm từng bước chuyển hóa chế độ chính trị ở nước ta diễn ra mạnh mẽ. Hàng năm, Bộ Công an rà soát, phát hiện hơn 7.500 nguồn khởi phát thông tin xấu độc, thu hút hơn 83 triệu lượt tiếp cận, tương tác thông tin, tập trung công kích, chống phá. Các hội nhóm "trái chiều", bảo hiểm, bất động sản bị các tổ chức phản động lưu vong kích động, đã tổ chức tập trung đông người "đòi quyền lợi" và hoạt động chống phá nhân các sự kiện, ngày lễ lớn của đất nước.

Thứ tư, hoạt động sử dụng công nghệ cao để thực hiện hành vi phạm tội, xâm phạm trật tự, an toàn xã hội diễn ra ngày càng phức tạp, gây bức xúc trong xã hội, gây thiệt hại lớn về tài sản cho người dân, nhất là hoạt động lừa đảo, chiếm đoạt tài sản, đánh bạc và tổ chức đánh bạc, truyền bá văn hóa phẩm đồi trụy, mua bán vũ khí, vật liệu nổ, ma túy, bằng cấp giả. Đặc biệt, các nhóm tội phạm người nước ngoài có xu hướng dịch chuyển sang địa bàn Việt Nam để thực hiện hành vi phạm tội với nhiều thủ đoạn hoạt động mới tinh vi hơn, tập trung ở các tỉnh, thành phố lớn, khu du lịch, vùng ven biển có vị trí chiến lược, thiết yếu về an ninh quốc phòng như thành phố Hồ Chí Minh, Hải Phòng, Quảng Ninh, Nha Trang, Đà Nẵng... Một số đối tượng người Trung Quốc còn móc nối, cấu kết với đối tượng người Việt Nam để lừa đảo, lôi kéo người Việt Nam sang

Campuchia phạm tội sử dụng công nghệ cao, dưới hình thức giới thiệu "việc nhẹ, lương cao".

Thực tế, trong 06 tháng đầu năm 2025, phát hiện 25 vụ việc liên quan hệ thống thông tin của một số cơ quan, đơn vị tồn tại điểm yếu, lỗ hổng bảo mật nghiêm trọng, xảy ra tình trạng lây nhiễm mã độc; lộ mất tài khoản quản trị, tài khoản người dùng ; 56 vụ việc liên quan hoạt động quảng cáo, rao bán thông tin, dữ liệu cá nhân trên các diễn đàn hội nhóm, trang mạng tin tặc với gần 110 triệu bản ghi. Triển khai Đề án 06 của Chính phủ, Bộ Công an tiến hành kiểm tra, đánh giá an ninh mạng hệ thống tin tại 07 ban, bộ, ngành, địa phương kết nối Cơ sở dữ liệu quốc gia về dân cư và hệ thống định danh xác thực điện tử VneID , phát hiện 1.315 lỗ hổng bảo mật mức độ nghiêm trọng, 4.095 lỗ hổng bảo mật mức độ cao tại các máy chủ hệ thống. Một trong những nguyên nhân dẫn đến thực trạng trên là do sự bất cập, thiếu đồng bộ trong hệ thống chính sách, pháp luật về lĩnh vực an ninh mạng.

Bối cảnh và tình hình trên đã đặt ra yêu cầu cấp bách là tiếp tục nhanh chóng hoàn thiện thể chế, chính sách pháp luật làm nền tảng vững chắc để bảo vệ an ninh đối với hệ thống thông tin và hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; hoạt động bảo vệ an ninh mạng; tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng; kinh doanh sản phẩm, dịch vụ an ninh mạng; điều kiện bảo đảm an ninh mạng...

II. MỤC ĐÍCH BAN HÀNH, QUAN ĐIỂM XÂY DỰNG DỰ THẢO LUẬT

1. Mục đích ban hành

Chính phủ đề xuất xây dựng Luật An ninh mạng nhằm:

- Bảo đảm tính thống nhất, đồng bộ của hệ thống pháp luật, loại bỏ sự chồng chéo, mâu thuẫn giữa hai luật hiện hành, tạo khung pháp lý rõ ràng, minh bạch, đáp ứng yêu cầu quản lý và bảo vệ không gian mạng.

- Nâng cao hiệu quả của hoạt động bảo đảm an ninh mạng, kết hợp chặt chẽ các biện pháp bảo vệ hệ thống thông tin, dữ liệu cá nhân, phòng chống tấn công mạng với các giải pháp bảo đảm an ninh quốc gia trên không gian mạng.

- Tạo điều kiện thuận lợi cho tổ chức, doanh nghiệp và cá nhân trong việc tuân thủ pháp luật, giảm thiểu thủ tục hành chính, đồng thời bảo vệ quyền lợi hợp pháp, thúc đẩy môi trường số an toàn, phát triển kinh tế số bền vững.

- Hoàn thiện cơ chế phòng thủ, giám sát, cảnh báo và ứng phó với các nguy cơ, sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng quốc gia, tăng cường năng lực phòng ngừa và khắc phục hậu quả của các cuộc tấn công mạng.

- Đáp ứng yêu cầu hội nhập quốc tế, phù hợp với các cam kết, chuẩn mực quốc tế về an ninh mạng, thúc đẩy nghiên cứu, phát triển công nghệ và nâng cao năng lực cạnh tranh của Việt Nam trong lĩnh vực an ninh mạng.

2. Quan điểm xây dựng dự án, dự thảo Luật

Dự án Luật An ninh mạng được xây dựng trên cơ sở sự hợp nhất quy định của Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) và Luật An ninh mạng năm 2018 và bổ sung một số quy định về những vấn đề cấp bách đang phát sinh, tác động lớn đến đời sống xã hội do sự phát triển vượt bậc của khoa học và công nghệ trong thời đại mới. Quan điểm xây dựng dự án Luật gồm :

- Luật An ninh mạng là luật khung, trên cơ sở sự hợp nhất quy định hiện hành của Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) và Luật An ninh mạng năm 2018.

- Luật An ninh mạng là luật kế thừa quan điểm pháp lý đã có tại Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) và Luật An ninh mạng năm 2018, bổ sung các khoảng trống pháp lý để hoàn thiện pháp luật về an ninh mạng.

- Nội dung Luật An ninh mạng bãi bỏ những quy định trùng lặp tại Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) và Luật An ninh mạng năm 2018 và các văn bản pháp lý khác có liên quan, không làm thay đổi về trách nhiệm quản lý nhà nước của các bộ, ngành trong các lĩnh vực và không làm thay đổi trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

- Luật An ninh mạng đẩy mạnh phân quyền cho Chính phủ và các cơ quan trong bộ máy nhà nước để cụ thể hóa các quy định của luật; thực hiện phân cấp bảo đảm phù hợp với năng lực tổ chức thực hiện của từng cơ quan, tổ chức, chính quyền địa phương các cấp và kịp thời đáp ứng yêu cầu phát triển kinh tế - xã hội trong từng giai đoạn.

- Nội dung Luật An ninh mạng bảo đảm việc thực hiện chủ trương phân quyền, phân cấp; giải quyết vấn đề bất cập, phát sinh từ thực tiễn; vấn đề mới, xu hướng mới; yêu cầu quản lý nhà nước và khuyến khích sáng tạo, khơi thông mọi nguồn lực, thúc đẩy phát triển kinh tế - xã hội.

III. PHẠM VI ĐIỀU CHỈNH CỦA LUẬT

Dự án Luật An ninh mạng dự kiến quy định về hoạt động bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội và bảo vệ quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng; bảo đảm an ninh thông tin, an toàn hệ thống thông tin; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

Dự án Luật An ninh mạng dự kiến áp dụng với cơ quan, tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng tại Việt Nam; tổ chức, cá nhân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng.

IV. VỀ TÍNH THỐNG NHẤT VỚI CÁC CHỦ TRƯƠNG, ĐƯỜNG LỐI CỦA ĐẢNG, VĂN BẢN QUY PHẠM PHÁP LUẬT, ĐIỀU ƯỚC QUỐC TẾ CÓ LIÊN QUAN ĐẾN DỰ THẢO LUẬT

Nội dung dự án Luật liên quan đến nhiều chủ trương của Đảng như: Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược Bảo vệ Tổ quốc trên không gian mạng, Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia; Nghị quyết 44-NQ/TW ngày 24/11/2023 của Ban Chấp hành Trung ương Đảng khóa XIII về chiến lược bảo vệ Tổ quốc trong tình hình mới; Nghị quyết số 66-NQ/TW ngày 30/4/2025 của Bộ Chính trị về đổi mới công tác xây dựng và thi hành pháp luật đáp ứng yêu cầu phát triển đất nước trong kỷ nguyên mới; Nghị quyết 68-NQ/TW ngày 04/5/2025 của Bộ Chính trị về phát triển kinh tế tư nhân...

Qua rà soát, thống kê các văn bản quy phạm pháp luật chịu sự điều chỉnh sau sắp xếp, điều chuyển chức năng, nhiệm vụ bảo đảm an toàn thông tin từ Bộ Thông tin và Truyền thông, dự kiến có 54 văn bản quy phạm pháp luật (10 Luật; 16 Nghị định của Chính phủ; 01 Quyết định của Thủ tướng, 27 Thông tư của Bộ trưởng) trong lĩnh vực an ninh mạng và an toàn thông tin cần điều chỉnh, bổ sung, hợp nhất

Nội dung của dự thảo Luật được bảo đảm tính thống nhất với các văn bản quy phạm pháp luật liên quan và tương thích, phù hợp với các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên; cụ thể: Công ước Quốc tế về các Quyền dân sự và chính trị (ICCPR); Công ước về quyền trẻ em nam 1989 (CRC), Bình luận chung số 16 về quyền riêng tư tại Điều 17 Công ước ICCPR của Ủy ban Nhân quyền; Công ước Liên hợp quốc về chống tội phạm mạng[1], Công ước của Liên hợp quốc về chống tội phạm có tổ chức xuyên quốc gia (CPC); Công ước quốc tế các quyền kinh tế, xã hội và văn hoá (ICESCR).

V. QUÁ TRÌNH XÂY DỰNG DỰ ÁN LUẬT

1. Chính phủ giao Bộ Công an chủ trì, phối hợp với các bộ, ngành, cơ quan liên quan xây dựng dự án Luật.

2. Hồ sơ dự án Luật đã được Bộ Công an xây dựng theo đúng quy định của Luật Ban hành văn bản quy phạm pháp luật

3. Ngày 22/8/2025, Bộ Tư pháp có Báo cáo số 366/BCTĐ-BTP về việc thẩm định đối với Hồ sơ dự án Luật. Bộ Công an đã có Báo cáo giải trình, tiếp thu ý kiến thẩm định của Bộ Tư pháp.

---

[1] Đây là Công ước đa phương toàn cầu đầu tiên được tổ chức ký tại Hà Nội vào tháng 10/2025 (dự kiến sẽ có tên gọi khác là Công ước Hà Nội) và Việt Nam sẽ là một trong những quốc gia thành viên của Công ước này.

4. Ngày 29/8/2025, Bộ Công an có Tờ trình số ...../TTr-BCA trình Chính phủ dự án Luật An ninh mạng.

VI. BỐ CỤC VÀ NỘI DUNG CƠ BẢN CỦA DỰ THẢO LUẬT

1. Bố cục

Dự thảo Luật gồm 09 chương với 63 điều, cụ thể như sau:

- Chương I. Những quy định chung gồm 10 điều, từ Điều 1 đến Điều 10 quy định về phạm vi điều chỉnh; đối tượng áp dụng; giải thích từ ngữ; chính sách của Đảng, Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; biện pháp bảo vệ an ninh mạng; bảo vệ không gian mạng quốc gia; hợp tác quốc tế về an ninh mạng; các hành vi bị nghiêm cấm về an ninh mạng; xử lý vi phạm pháp luật về an ninh mạng.

- Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin và hệ thống thông tin quan trọng về an ninh quốc gia gồm 11 điều, từ Điều 11 đến Điều 21 quy định về phân loại cấp độ hệ thống thông tin; nhiệm vụ bảo vệ hệ thống thông tin; biện pháp bảo vệ hệ thống thông tin; hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

- Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng với 10 điều, từ Điều 22 đến Điều 31 quy định về: phòng ngừa, xử lý thông tin trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội; phòng ngừa, xử lý thông tin trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội; phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; phòng, chống xâm hại trẻ em trên không gian mạng; phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng; ngăn chặn xung đột thông tin trên mạng.

- Chương IV. Hoạt động bảo vệ an ninh mạng gồm 06 điều, từ Điều 32 đến Điều 37 quy định về phân loại thông tin; quản lý gửi thông tin trên mạng;

triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương; bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế; bảo đảm an ninh thông tin trên không gian mạng; bảo đảm an ninh dữ liệu.

- Chương V. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng gồm 03 điều, từ Điều 38 đến Điều 40 quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng; quản lý tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng; đánh giá hợp chuẩn, hợp quy về an ninh mạng.

- Chương VI. Kinh doanh sản phẩm, dịch vụ an ninh mạng gồm 04 điều, từ Điều 41 đến Điều 44 quy định về sản phẩm, dịch vụ an ninh mạng; cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng; nguyên tắc quản lý xuất, nhập khẩu sản phẩm, dịch vụ an ninh mạng.

- Chương VI. Điều kiện bảo đảm an ninh mạng gồm 10 điều, từ Điều 45 đến Điều 54 quy định về nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; lực lượng chuyên trách bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng; tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; giáo dục bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; phổ biến kiến thức về an ninh mạng; yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng; kinh phí bảo vệ an ninh mạng.

- Chương VIII. Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an ninh mạng gồm 07 điều, từ Điều 55 đến Điều 61 quy định về trách nhiệm của Bộ Công an; trách nhiệm của Bộ Quốc phòng; trách nhiệm của Ban Cơ yếu Chính phủ; trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh; trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng.

- Chương IX. Điều khoản thi hành gồm 02 điều, Điều 62 và Điều 63 quy định về hiệu lực thi hành và điều khoản chuyển tiếp.

2. Nội dung cơ bản của dự thảo Luật

Dự thảo Luật kế thừa 33 điều của Luật An ninh mạng năm 2018 (trong đó giữ nguyên 29 điều, sửa đổi, bổ sung 04 điều), kế thừa 19 điều của Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) (trong đó giữ nguyên 15 điều, sửa đổi, bổ sung 04 điều); hợp nhất nội dung của 08 điều luật của 02 luật nêu trên; bổ sung 03 điều. Cụ thể như sau:

- Nhóm 33 điều luật kế thừa của Luật An ninh mạng năm 2018: Biện pháp bảo vệ an ninh mạng; Hệ thống thông tin quan trọng về an ninh quốc gia; Bảo đảm an ninh thông tin trên không gian mạng; Phòng ngừa, xử lý thông tin trên không gian mạng xâm phạm an ninh quốc gia; Phòng ngừa, xử lý thông tin

trên không gian mạng xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân; Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia; Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để vi phạm pháp luật về trật tự, an toàn xã hội; Phòng, chống xâm hại trẻ em trên không gian mạng; Phòng, chống tấn công mạng; Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; Đấu tranh bảo vệ an ninh mạng; Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; Nghiên cứu, phát triển an ninh mạng; Nâng cao năng lực tự chủ về an ninh mạng; Bảo đảm nguồn nhân lực bảo vệ an ninh mạng; Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; Giáo dục bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; Phổ biến kiến thức về an ninh mạng; Kinh phí bảo vệ an ninh mạng; Trách nhiệm của tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế trong bảo vệ an ninh mạng; Trách nhiệm của Bộ Công an; Trách nhiệm của Bộ Quốc phòng; Trách nhiệm của Ban Cơ yếu Chính phủ; Trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh; Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng; Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng.

- Nhóm 19 điều luật kế thừa của Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018): Đối tượng áp dụng; Phân loại cấp độ hệ thống thông tin; Nhiệm vụ bảo vệ hệ thống thông tin; Biện pháp bảo vệ hệ thống thông tin; Trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; Quản lý gửi thông tin trên mạng; Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an ninh thông tin; Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại; Ngăn chặn xung đột thông tin trên mạng; Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng; Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng; Đánh giá hợp chuẩn, hợp quy về an ninh mạng; Sản phẩm, dịch vụ an ninh mạng; Cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; Cấp Giấy chứng nhận hành nghề cung cấp sản phẩm, dịch vụ an ninh mạng; Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng; Nguyên tắc quản lý xuất, nhập khẩu sản phẩm, dịch vụ an ninh mạng; Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng; Quản lý nhà nước về an ninh mạng.

- Nhóm 08 điều luật hợp nhất: Phạm vi điều chỉnh; Chính sách của Nhà nước về an ninh mạng; Nguyên tắc bảo vệ an ninh mạng; Hợp tác quốc tế về an ninh mạng; Các hành vi bị nghiêm cấm về an ninh mạng; Xử lý vi phạm pháp luật về an ninh mạng; Điều khoản chuyển tiếp; Hiệu lực thi hành.

- Nhóm 03 điều được bổ sung: Bảo đảm an ninh dữ liệu; Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng; Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng.

3. Về một số vấn đề mới

Với các nội dung mới, nội dung được sửa đổi, bổ sung trong dự thảo Luật, Bộ Công an báo cáo cụ thể như sau:

An ninh dữ liệu là vấn đề mới, việc bổ sung trong dự thảo Luật nhằm cụ thể hóa chủ trương chính sách, chỉ đạo của lãnh đạo Đảng, Nhà nước (cụ thể là Nghị quyết 57). Các đối tượng cần được bảo vệ an ninh dữ liệu rất đa dạng, bao gồm dữ liệu cá nhân, dữ liệu tổ chức, dữ liệu hệ thống, dữ liệu trong quá trình truyền tải, hạ tầng công nghệ và quyền riêng tư của người dùng. Mỗi loại dữ liệu đều có các yêu cầu bảo vệ riêng và việc thực hiện các biện pháp bảo vệ phù hợp sẽ đảm bảo sự an toàn và bảo mật cho các thông tin quan trọng này.

Các nội dung được hợp nhất, sửa đổi, bổ sung trong dự thảo Luật nhằm bảo đảm phù hợp, thống nhất với cơ cấu, tổ chức bộ máy của hệ thống chính trị, được quy định tại các văn bản luật khác như: Nghị quyết số 203/2025/QH15 ngày 16/6/2025 của Quốc hội sửa đổi, bổ sung một số điều của Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam; Luật Tổ chức chính quyền địa phương; Nghị định số 02/2025/NĐ-CP ngày 18/02/2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an...

VII. DỰ KIẾN NGUỒN LỰC, ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THI HÀNH LUẬT

1. Để bảo đảm triển khai thi hành Luật An ninh mạng cần bảo đảm các nguồn lực sau đây:

- Kinh phí xây dựng Luật và các văn bản quy định chi tiết và hướng dẫn thi hành dự kiến khoảng 4.000.000.000 đồng.

- Kinh phí để tổ chức triển khai thi hành Luật và các văn bản quy định chi tiết và hướng dẫn thi hành trên thực tế (biên soạn tài liệu, tổ chức hội nghị tập huấn trong cơ quan có chức năng quản lý nhà nước về thi hành án hình sự, phổ biến đến quần chúng nhân dân…) khoảng 2.000.000.000 đồng.

Đây là khoản chi cần thiết và tất yếu để triển khai thi hành Luật và nâng cao hiệu quả công tác thi hành án hình sự trong thời gian tới. Nguồn kinh phí bảo đảm nêu trên sẽ được cân đối từ ngân sách Nhà nước và nguồn kinh phí hợp pháp khác; ngân sách Nhà nước bảo đảm trên thực tế là khả thi.

2. Để bảo đảm triển khai thi hành Luật An ninh mạng sau khi được Quốc hội thông qua, nguồn nhân lực bảo đảm là đội ngũ nhân lực hiện đang được giao thực hiện nhiệm vụ bảo vệ an ninh mạng, không làm tăng tổ chức bộ máy và biên chế hưởng lương từ ngân sách nhà nước.

Trên đây là Tờ trình về dự án Luật An ninh mạng, Bộ Công an kính trình Chính phủ xem xét, quyết định./.

(Xin gửi kèm theo: (1) Dự thảo Luật; (2) Báo cáo thẩm định của Bộ Tư pháp; (3) Báo cáo giải trình, tiếp thu ý kiến thẩm định của Bộ Tư pháp; (4) Bản tổng hợp, tiếp thu, giải trình ý kiến góp ý của các bộ, ngành, địa phương; (5) Báo cáo đánh giá tác động chính sách; (6) Báo cáo về rà soát các văn bản quy phạm pháp luật liên quan đến dự án Luật; (7) Báo cáo về lồng ghép vấn đề bình đẳng giới trong dự án Luật; (8) Báo cáo đánh giá tác động thủ tục hành chính; (9) Dự thảo văn bản quy định chi tiết Luật; (10) Bản so sánh Luật).

Nơi nhận:
- Như trên;
- Thủ tướng Chính phủ;
- Các Phó Thủ tướng Chính phủ;
- Ủy ban Thường vụ Quốc hội;
- Ủy ban Pháp luật và Tư pháp của Quốc hội;
- Văn phòng Quốc hội;
- Bộ Công an;
- Bộ Quốc phòng;
- Bộ Tư pháp;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Văn phòng Chính phủ: BTCN, các PCN, trợ lý TTg, TGĐ cổng TTĐT; Các vụ, cục: NC, QHĐP, PL, TH, KSKT;
- Lưu: VT, NC (02).

BỘ TRƯỞNG

Đại tướng Lương Tam Quang

MỤC LỤC

QUỐC HỘI	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
Luật số: /2025/QH15	**Độc lập – Tự do – Hạnh phúc**

DỰ THẢO NGÀY 29.8.2025

LUẬT
AN NINH MẠNG

Căn cứ Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam đã được sửa đổi, bổ sung một số điều theo Nghị quyết số 203/2025/QH15;

Quốc hội ban hành Luật An ninh mạng.

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Luật này quy định về hoạt động bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội và bảo vệ quyền, lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân trên không gian mạng; bảo đảm an ninh thông tin, an ninh dữ liệu, an toàn hệ thống thông tin; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

Điều 2. Đối tượng áp dụng

Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng tại Việt Nam.

Điều 3. Giải thích từ ngữ

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

1. An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; bảo đảm an ninh dữ liệu; bảo vệ thông tin, hệ thống thông tin, nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

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

3. Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

4. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

5. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng.

6. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

7. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

8. Phần cứng độc hại là các bộ phận vật lý của hệ thống máy tính, hệ thống thông tin, được tạo ra có chủ đích, nằm ngoài thiết kế và quy cách thiết bị tiêu chuẩn, có thể được điều khiển hoặc thực hiện tính năng can thiệp vào phần mềm, phần cứng hệ thống, gây ra tác động bất bình thường cho một phần hay toàn bộ hệ thống máy tính, hệ thống thông tin, hoặc đánh cắp thông tin, dữ liệu trái phép lưu trữ trong hệ thống máy tính, hệ thống thông tin, hoặc gây ngừng trệ, tê liệt, phá hoại hệ thống tùy theo mục đích thiết kế.

9. Nhật ký hệ thống là hệ thống được thiết lập có chức năng ghi nhận, lưu trữ và có thể trích xuất dữ liệu phản ánh những sự kiện liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh mạng của hệ thống và dữ liệu do người dùng tạo ra trong quá trình sử dụng hệ thống, truy cập dịch vụ Internet.

10. Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự.

11. Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

12. Khủng bố mạng là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.

13. Gián điệp mạng là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác nhằm chiếm đoạt, thu thập trái phép tài liệu, thông tin bí mật, tài nguyên thông tin của cơ quan, tổ chức Nhà nước hoặc nhằm mục đích gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

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

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

16. Xung đột thông tin là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

17. Tình huống nguy hiểm về an ninh mạng là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

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

19. Mật mã dân sự là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

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

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

Điều 4. Chính sách của Nhà nước về an ninh mạng

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

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

3. Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng, bảo đảm nguồn nhân lực trình độ cao cho bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng; có cơ chế đặc thù, chính sách ưu đãi để huy động, thu hút và sử dụng nhân tài trong lĩnh vực an ninh mạng.

4. Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công

nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng.

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

Điều 5. Nguyên tắc bảo vệ an ninh mạng

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng.

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

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

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

5. Triển khai hoạt động bảo vệ an ninh mạng thường xuyên, liên tục đối với cơ sở hạ tầng không gian mạng quốc gia nhằm bảo vệ vững chắc nền tảng của công cuộc chuyển đổi số quốc gia, hướng đến mục tiêu tự chủ về công nghệ an ninh mạng, ưu tiên trong những lĩnh vực chiến lược.

6. Chủ động áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng quốc gia; bảo đảm hệ thống thông tin quan trọng quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

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

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

Điều 6. Biện pháp bảo vệ an ninh mạng

1. Biện pháp bảo vệ an ninh mạng bao gồm:

a) Thẩm định an ninh mạng;

b) Đánh giá điều kiện an ninh mạng;

c) Kiểm tra an ninh mạng;

d) Giám sát an ninh mạng;

đ) Ứng phó, khắc phục sự cố an ninh mạng;

e) Đấu tranh bảo vệ an ninh mạng;

g) Sử dụng mật mã để bảo vệ thông tin mạng;

h) Sử dụng giải pháp kỹ thuật để bảo vệ dữ liệu; bảo vệ thông tin, hệ thống thông tin; ngăn chặn thông tin vi phạm pháp luật.

i) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

k) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

l) Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng;

m) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật;

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

p) Biện pháp khác theo quy định của pháp luật về bảo vệ an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

2. Chính phủ quy định chi tiết về nội dung, trình tự, thủ tục, thẩm quyền áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm n và điểm o khoản 1 Điều này.

Điều 7. Bảo vệ không gian mạng quốc gia

Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.

Điều 8. Hợp tác quốc tế về an ninh mạng

1. Hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng, cùng có lợi và tuân thủ Hiến pháp, pháp luật Việt Nam, điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

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

a) Chia sẻ thông tin, dữ liệu và cảnh báo sớm về nguy cơ, sự cố, tấn công mạng ảnh hưởng đến an ninh mạng;

b) Xây dựng khuôn khổ pháp lý, chính sách và cơ chế phối hợp trong bảo vệ an ninh mạng; ký kết, tham gia thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng;

c) Đào tạo, tư vấn, chia sẻ kinh nghiệm và nâng cao năng lực chuyên môn, kỹ thuật trong lĩnh vực an ninh mạng;

d) Phòng, chống tội phạm sử dụng công nghệ cao; phối hợp điều tra, xử lý vi phạm pháp luật và tội phạm sử dụng công nghệ cao có yếu tố nước ngoài;

đ) Nghiên cứu, phát triển, chuyển giao công nghệ, sản phẩm, giải pháp kỹ thuật phục vụ công tác bảo vệ an ninh mạng;

e) Tổ chức hội nghị, hội thảo, diễn đàn quốc tế và triển khai các chương trình, dự án hợp tác quốc tế về an ninh mạng;

g) Hoạt động hợp tác quốc tế khác về an ninh mạng.

3. Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.

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

Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng.

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

4. Hoạt động hợp tác quốc tế về an ninh mạng của Bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.

Điều 9. Các hành vi bị nghiêm cấm về an ninh mạng

1. Sử dụng không gian mạng để đăng tải, phát tán thông tin có nội dung:

a) Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

b) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

c) Bịa đặt, vu khống, vu cáo sai sự thật, xúc phạm danh dự, uy tín, nhân phẩm của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

d) Sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.

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

a) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Kích động, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

c) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật Nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc;

d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

đ) Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

e) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức Nhà nước;

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

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

i) Thực hiện hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

3. Thực hiện tấn công mạng; khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin

4. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

5. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

6. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

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

Điều 10. Xử lý vi phạm pháp luật về an ninh mạng

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

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

Điều 11. Phân loại cấp độ hệ thống thông tin

1. Phân loại cấp độ hệ thống thông tin là việc xác định cấp độ an ninh mạng của hệ thống thông tin để áp dụng biện pháp bảo vệ tương ứng, phù hợp theo từng cấp độ tăng dần từ 1 đến 5.

2. Hệ thống thông tin được phân loại theo cấp độ như sau:

a) Cấp độ 1 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

b) Cấp độ 2 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

c) Cấp độ 3 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;

d) Cấp độ 4 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;

đ) Cấp độ 5 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới chủ quyền, lợi ích, quốc phòng, an ninh quốc gia.

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

Điều 12. Nhiệm vụ bảo vệ hệ thống thông tin

1. Nội dung nhiệm vụ bảo vệ hệ thống thông tin, bao gồm:

a) Xác định cấp độ an ninh mạng của hệ thống thông tin và hệ thống thông tin quan trọng quốc gia.

b) Đánh giá và quản lý rủi ro an ninh mạng hệ thống thông tin.

c) Đôn đốc, giám sát, kiểm tra công tác bảo vệ an ninh mạng hệ thống thông tin.

d) Tổ chức triển khai các biện pháp bảo vệ an ninh mạng hệ thống thông tin.

e) Thực hiện chế độ báo cáo theo quy định.

g) Tổ chức tuyên truyền, nâng cao nhận thức về an ninh mạng.

2. Chủ quản hệ thống thông tin thuộc Cấp độ 1 và Cấp độ 2 tự chịu trách nhiệm thực hiện các nội dung quy định tại Khoản 1 Điều này.

3. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4, Cấp độ 5 phải thực hiện đầy đủ các nội dung nhiệm vụ quy định tại Khoản 1 Điều này.

Điều 13. Biện pháp bảo vệ hệ thống thông tin

1. Các biện pháp bảo vệ đối với hệ thống thông tin, bao gồm:

a) Ban hành quy định về bảo đảm an ninh mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin.

b) Thẩm định an ninh mạng đối với hồ sơ, thiết kế của hệ thống thông tin.

c) Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin.

d) Áp dụng biện pháp quản lý theo tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng, nghiên cứu xây dựng hệ thống tường lửa quốc gia để phòng, chống nguy cơ, khắc phục sự cố an ninh mạng.

đ) Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng.

e) Thực hiện giám sát an ninh mạng.

g) Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin

2. Chủ quản hệ thống thông tin thuộc Cấp độ 1 và Cấp độ 2 có thể lựa chọn áp dụng đầy đủ hoặc một số biện pháp quy định tại khoản 1 Điều này tùy theo nhu cầu và khả năng đáp ứng thực tế.

3. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4, Cấp độ 5 phải áp dụng đầy đủ các biện pháp quy định tại khoản 1 Điều này.

4. Chính phủ quy định chi tiết về nội dung nhiệm vụ và biện pháp bảo vệ đối với hệ thống thông tin theo cấp độ và đối với hệ thống thông tin quan trọng về an ninh quốc gia, được quy định tại khoản 1 Điều 12 và khoản 1 Điều 13 Luật này.

Điều 14. Hệ thống thông tin quan trọng về an ninh quốc gia

1. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin thuộc Cấp độ 5; hoặc hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4 và đáp ứng một số tiêu chí nhất định theo quy định của Chính phủ.

2. Danh mục hệ thống thông tin quan trọng về an ninh quốc gia là danh sách hệ thống thông tin quan trọng về an ninh quốc gia được xác lập, ban hành và áp dụng biện pháp bảo vệ tương xứng nhằm bảo đảm hoạt động ổn định của các lĩnh vực quan trọng, bao gồm:

a) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu;

b) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước;

c) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng;

d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái;

đ) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia;

e) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương;

g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí;

h) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

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

Bộ Công an chủ trì, phối hợp bộ, ngành có liên quan xây dựng Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trình Thủ tướng Chính phủ ban hành, sửa đổi, bổ sung.

Điều 15. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

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

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

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

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

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

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

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

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

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

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

Điều 16. Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

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

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

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

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

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

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

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

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

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

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

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

Điều 17. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

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

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

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

c) Kiểm tra định kỳ hằng năm;

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

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

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

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

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

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

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

e) Nhân lực bảo vệ an ninh mạng.

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

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

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

b) Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ

hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin;

c) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước.

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

Ban Cơ yếu Chính phủ kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước;

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

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

Điều 18. Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

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

3. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Điều 19. Trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

a) Thực hiện quy định tại khoản 1 Điều 12 và khoản 1 Điều 13 Luật này;

b) Khi thiết lập, mở rộng và nâng cấp hệ thống thông tin quan trọng về a ninh quốc gia phải thực hiện kiểm định an ninh mạng trước khi đi vào vận hành, khai thác; định kỳ hằng năm, tự kiểm tra, đánh giá an ninh mạng hệ thống thông tin quan trọng về an ninh quốc gia; và thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

c) Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền trong việc thường xuyên thực hiện giám sát an ninh mạng; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng; đề ra phương án ứng phó, khắc phục khẩn cấp;

d) Xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền;

đ) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong việc thực hiện kiểm tra an ninh mạng đột xuất.

2. Bộ Công an có trách nhiệm sau đây đối với các hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu do Bộ Quốc phòng và Ban Cơ yếu Chính phủ quản lý theo quy định của pháp luật:

a) Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

b) Đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

c) Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia;

d) Thực hiện giám sát an ninh mạng; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

đ) Chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia, tham gia ứng phó, khắc phục sự cố khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng;

e) Chủ trì, phối hợp Ban Cơ yếu Chính phủ trong triển khai các biện bảo bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia có sử dụng giải pháp, sản phẩm mật mã của ngành Cơ yếu Việt Nam để bảo vệ bí mật nhà nước.

3. Bộ Quốc phòng chủ trì thẩm định, đánh giá, kiểm tra an ninh mạng đột xuất và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia do Bộ Quốc phòng quản lý.

4. Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã để bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định, đánh giá, kiểm tra an ninh mạng đột xuất, giám sát an ninh mạng và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin cơ yếu do Ban Cơ yếu Chính phủ quản lý.

Điều 20. Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

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

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

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

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

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

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

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

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

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

2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền.

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

a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; tham gia ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng;

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

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

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

Điều 21. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

1. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trong trường hợp sau đây:

a) Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội;

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

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

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

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

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

3. Chủ quản hệ thống thông tin có trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức trong các trường hợp quy định tại khoản 1 Điều này.

5. Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ.

Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin.

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

7. Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng quy định tại Điều này.

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

Điều 22. Phòng ngừa, xử lý thông tin trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội

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

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

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

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Thông tin trên không gian mạng có nội dung xâm phạm an ninh lãnh thổ, lợi ích của Nhà nước, phá hoại chính sách kinh tế - xã hội, cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Phản ánh sai lệch, không chính xác về đường biên giới quốc gia chủ quyền lãnh thổ quốc gia Việt Nam; đăng tải, truyền đưa hình ảnh sai lệch, không chính xác, không đầy đủ về bản đồ Việt Nam hoặc thể hiện sai chủ quyền quốc gia Việt Nam;

b) Tuyên truyền gây tổn hại trực tiếp hoặc gián tiếp đến quyền, lợi ích hợp pháp của Nhà nước về chính trị, kinh tế, xã hội, uy tín quốc tế;

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

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

4. Thông tin trên không gian mạng có nội dung phá hoại chính sách đoàn kết bao gồm:

a) Gây mâu thuẫn, chia rẽ giữa các tầng lớp nhân dân, giữa nhân dân với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội;

b) Kích động, gây hận thù, kỳ thị, chia rẽ, ly khai dân tộc, xâm phạm quyền bình đẳng trong cộng động các dân tộc Việt Nam;

c) Kích động, gây mâu thuẫn, chia rẽ người theo tôn giáo với người không theo tôn giáo, giữa người theo các tôn giáo khác nhau, chia rẽ các tín đồ tôn giáo với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội;

d) Phá hoại, cản trở việc thực hiện chính sách đoàn kết quốc tế.

5. Thông tin trên không gian mạng có nội dung xâm phạm quyền, lợi ích hợp pháp của cá nhân bao gồm:

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

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

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

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

c) Mạo danh, giả mạo thông tin, hình ảnh, giọng nói của cá nhân, gây ảnh hưởng đến uy tín, danh dự, nhân phẩm của cá nhân.

6. Thông tin trên không gian mạng có nội dung xâm phạm quyền, lợi ích hợp pháp của tổ chức bao gồm:

a) Loan truyền thông tin xuyên tạc, bịa đặt, sai sự thật, gây ảnh hưởng đến uy tín, hoạt động bình thường của tổ chức;

b) Kêu gọi, vận động, xúi giục tẩy chay sản phẩm, dịch vụ, hàng hóa, nhãn hàng, thương hiệu của tổ chức, doanh nghiệp, gây thiệt hại về vật chất, uy tín của doanh nghiệp, tổ chức;

c) Mạo danh, giả mạo thông tin, hình ảnh, làm nhái sản phẩm, nhãn hiệu hàng hóa, thương hiệu của tổ chức, doanh nghiệp bằng cách sử dụng các tiện ích công nghệ, gây ảnh hưởng đến uy tín của tổ chức, doanh nghiệp.

7. Chủ quản hệ thống thông tin, doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung quy định tại các khoản khoản 1, 2, 3, 4, 5 và 6 Điều này trên hệ thống thông tin thuộc phạm vi quản lý hoặc khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng.

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

9. Doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin có trách nhiệm phối hợp với cơ quan chức năng xử lý

thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4, 5 và 6 Điều này.

10. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4, 5 và 6 Điều này phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật.

Điều 23. Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng

1. Hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm:

a) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng;

c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư;

d) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;

đ) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

e) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.

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

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

b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này;

c) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà

nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

3. Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước.

4. Bộ Công an có trách nhiệm sau đây, trừ quy định tại khoản 5 và khoản 6 Điều này:

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

b) Kiểm tra an ninh mạng đối với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng quốc gia;

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

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

đ) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước theo quy định của pháp luật bảo vệ bí mật nhà nước và pháp luật cơ yếu; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao;

e) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng quốc gia;

g) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng quy định tại khoản 2 Điều 46 của Luật này.

5. Bộ Quốc phòng có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin quân sự.

6. Ban Cơ yếu Chính phủ có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ; có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

Điều 24. Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội

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

a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3 và 4 Điều 22;

b) Thực hiện hành vi quy định tại khoản 1 Điều 23 của Luật này.

2. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để xâm phạm trật tự, an an toàn xã hội bao gồm:

a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 5 và 6 Điều 22 của Luật này;

b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; làm giả con dấu, tài liệu hoặc giấy tờ khác của cơ quan, tổ chức

d) Tuyên truyền, quảng cáo, mua bán trái phép vũ khí, vật liệu nổ, công cụ hỗ trợ, pháo nổ; ma túy, tiền chất ma túy, chất gây nghiện, chất hướng thần; động vật hoang dã, nguy cấp, quý, hiếm và các hàng hóa, dịch vụ khác thuộc danh mục cấm theo quy định của pháp luật; môi giới mại dâm; truyền bá văn hóa phẩm đồi trụy; lạm dụng tình dục trẻ em; quấy rối tình dục;

đ) Thiết lập, cung cấp dịch vụ hoặc hỗ trợ vận hành, kinh doanh, giao dịch, mua bán, tiếp thị trực tuyến cho sàn giao dịch, website, ứng dụng trái phép trên không gian mạng, bao gồm: sàn thương mại điện tử, website, ứng dụng bán hàng, cung cấp dịch vụ thương mại điện tử; sàn giao dịch dựa trên chỉ số các loại hàng hóa; sàn giao dịch tài sản số, kinh doanh theo phương thức đa cấp;

e) Sử dụng danh tính giả, thông tin của người khác, giấy tờ, hồ sơ giả để thành lập doanh nghiệp, thiết lập, đăng ký tài khoản ngân hàng, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và tài khoản số khác; thu thập, tàng trữ, trao đổi, mua bán, tặng cho, công khai hóa trái phép dữ liệu, thông tin tài khoản ngân hàng, thẻ ngân hàng, tài khoản ví điện tử, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và các loại tài khoản số khác;

g) Quảng cáo, buôn bán hàng giả, hàng hóa nhập lậu, không rõ nguồn gốc, xuất xứ; hàng hóa lưu thông trong nước bị áp dụng biện pháp khẩn cấp; hàng hóa quá hạn sử dụng;

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

l) Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao vi phạm pháp luật về trật tự, an toàn xã hội.

3. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, Bộ Quốc phòng và cơ quan chức năng liên quan có trách nhiệm thực hiện các biện pháp quy định tại khoản 1 Điều 6 của Luật này để đấu tranh, phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để vi phạm pháp luật về trật tự, an toàn xã hội.

4. Chính phủ quy định chi tiết về phòng, chống tội phạm sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao xâm phạm trật tự, an toàn xã hội.

Điều 25. Phòng, chống xâm hại trẻ em trên không gian mạng

1. Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia, tương tác trên không gian mạng.

2. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm: kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em hoặc xâm phạm đến trẻ em hoặc xâm phạm quyền trẻ em, quyền của người yếu thế; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em hoặc xâm phạm đến trẻ em hoặc xâm phạm đến quyền trẻ em; xây dựng, triển khai các hệ thống kỹ thuật hỗ trợ hoạt động ngăn chặn nội dung xâm hại trẻ em trên không gian mạng; điều phối các cơ quan, tổ chức, doanh nghiệp thực hiện ngăn chặn các nguồn phát tán thông tin xâm hại trẻ em trên không gian mạng; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

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

4. Cơ quan, tổ chức, cha mẹ, con cái, người giám hộ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, người yếu thế, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em.

5. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử

lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

Điều 26. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại

1. Cơ quan, tổ chức, cá nhân có trách nhiệm chủ động phòng ngừa, ngăn chặn phần mềm độc hại và thực hiện phòng ngừa, ngăn chặn theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền.

2. Chủ quản hệ thống thông tin quan trọng quốc gia triển khai hệ thống kỹ thuật nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời phần mềm độc hại.

3. Tổ chức, doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình và báo cáo cơ quan nhà nước có thẩm quyền theo quy định của pháp luật.

4. Doanh nghiệp cung cấp dịch vụ Internet có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền.

5. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh quốc gia.

Điều 27. Phòng, chống tấn công mạng

1. Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm:

a) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của không gian mạng;

c) Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử;

d) Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính;

đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng gây hại mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật;

e) Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

2. Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi quy định tại các điểm a, b, c, d và e khoản 1 Điều này đối với hệ thống thông tin thuộc phạm vi quản lý.

3. Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

4. Trách nhiệm phòng, chống tấn công mạng được quy định như sau:

a) Bộ Công an chủ trì, phối hợp với bộ, ngành, địa phương có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội trên phạm vi cả nước, trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Điều 28. Phòng, chống khủng bố mạng

1. Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật này và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng.

2. Chủ quản hệ thống thông tin thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng.

3. Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng.

4. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp vô hiệu hóa nguồn

khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra đối với hệ thống thông tin, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này.

5. Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự.

6. Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ.

Điều 29. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

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

a) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố;

b) Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia;

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

d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia;

đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng được quy định như sau:

a) Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng;

b) Doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

3. Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm:

a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng;

d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế;

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

g) Biện pháp khác theo quy định của Luật An ninh quốc gia.

4. Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau:

a) Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và áp dụng ngay các biện pháp quy định tại điểm a và điểm b khoản 3 Điều này;

b) Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể.

Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;

c) Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp quy định tại khoản 3 Điều này để xử lý tình huống nguy hiểm về an ninh mạng;

d) Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

Điều 30. Đấu tranh bảo vệ an ninh mạng

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

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

a) Giám sát thông tin mạng và phòng ngừa, đấu tranh, xử lý tổ chức, cá nhân có hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

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

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

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

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

Điều 31. Ngăn chặn xung đột thông tin trên mạng

1. Ngăn chặn xung đột thông tin trên mạng là việc thực hiện các biện pháp công nghệ, kỹ thuật để giám sát, phát hiện, cảnh báo, xác định nguồn gốc, chặn lọc, khắc phục và loại trừ xung đột thông tin trên mạng.

2. Nội dung ngăn chặn xung đột thông tin trên mạng bao gồm:

a) Giám sát, phát hiện, cảnh báo, xung đột thông tin trên mạng;

b) Xác định nguồn gốc xung đột thông tin trên mạng;

c) Chặn lọc, khắc phục và loại trừ xung đột thông tin trên mạng;

d) Thông tin, tuyên truyền, giáo dục và hợp tác quốc tế về ngăn chặn xung đột thông tin trên mạng.

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

a) Ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;

b) Ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng;

c) Loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài.

4. Chính phủ quy định chi tiết về ngăn chặn xung đột thông tin trên mạng.

Chương IV
HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Điều 32. Phân loại thông tin

1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo mức độ nhạy cảm của thông tin, theo tính chất và lĩnh vực của thông tin, theo tình trạng và sự thay đổi của thông tin, theo mức độ quyền truy cập để có biện pháp bảo vệ phù hợp.

2. Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Cơ quan, tổ chức sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải có trách nhiệm xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

Điều 33. Quản lý gửi thông tin trên mạng

1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin;

b) Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật.

3. Nhà cung cấp dịch vụ có trách nhiệm sau đây:

a) Tuân thủ quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của tổ chức, cá nhân.

b) Áp dụng biện pháp ngăn chặn, xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật.

c) Có phương thức để người tiếp nhận thông tin có khả năng từ chối việc tiếp nhận thông tin.

d) Cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ quản lý, bảo đảm an ninh mạng khi có yêu cầu.

đ) Áp dụng cơ chế kiểm soát tự động để kiểm soát việc gửi thông tin trên mạng.

e) Tăng cường bảo mật thông tin liên quan đến giao dịch trực tuyến để bảo đảm an toàn cho các giao dịch thông qua các phương thức xác thực đa yếu tố, mã hóa thông tin và bảo vệ thông tin tài chính của người dùng khi gửi, nhận thông tin giao dịch trực tuyến.

g) Cung cấp thông tin đầy đủ về quyền và nghĩa vụ của người tiếp nhận thông tin khi họ từ chối thông tin, cũng như các hậu quả và quyền lợi liên quan đến việc tiếp nhận hoặc từ chối nhận thông tin.

Điều 34. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;

b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý;

c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng;

d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ;

đ) Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin;

e) Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

2. Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

Điều 35. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế

1. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

2. Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế có trách nhiệm sau đây:

a) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền;

b) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.

Điều 36. Bảo đảm an ninh thông tin trên không gian mạng

1. Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải,

truyền đưa thông tin có nội dung được quy định tại khoản 1, 2, 3, 4 Điều 22 và khoản 1 Điều 23 Luật này và thông tin khác có nội dung xâm phạm an ninh quốc gia.

2. Doanh nghiệp trong nước và nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm sau đây:

a) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chậm nhất là 24 giờ khi có yêu cầu bằng văn bản hoặc thư điện tử, điện thoại hoặc một loại hình thức trao đổi khác đã được xác nhận để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, đe dọa tính mạng con người, yêu cầu cung cấp thông tin chậm nhất là 03 giờ.

b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm quy định của Luật này trên dịch vụ, kho ứng dụng hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của pháp luật (của Chính phủ); trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, yêu cầu ngăn chặn, xóa bỏ thông tin chậm nhất là 06 giờ.

c) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng đối với thông tin có nội dung quy định tại khoản 1, 2, 3, 4 Điều 20 và khoản 1, 2 Điều 21 Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an.

d) Lưu trữ thông tin cá nhân của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tạo ra, bao gồm: tên tài khoản, thời gian sử dụng dịch vụ, thông tin thanh toán phí sử dụng dịch vụ, địa chỉ IP truy cập và các dữ liệu liên quan khác trong suốt quá trình sử dụng đến 02 năm sau khi người dùng kết thúc việc sử dụng dịch vụ.

3. Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải áp dụng các biện pháp bảo vệ dữ liệu theo quy định của pháp luật và lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.

Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

4. Chính phủ quy định chi tiết khoản 2 và khoản 3 Điều này.

Điều 37. Bảo đảm an ninh dữ liệu

1. An ninh dữ liệu là sự bảo đảm an toàn, bí mật, khả dụng của dữ liệu chuyên ngành của cơ quan, tổ chức nhà nước; phòng, chống việc sử dụng, khai thác trái phép, chiếm đoạt, cố ý làm sai lệch, tiêu hủy dữ liệu chuyên ngành, phá hoại cơ sở dữ liệu chuyên ngành của cơ quan, tổ chức nhà nước, gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

2. Cơ quan, tổ chức, doanh nghiệp nhà nước thiết lập cơ sở, trung tâm, hệ thống lưu trữ dữ liệu chuyên ngành có trách nhiệm xây dựng và thực hiện hệ thống quản lý an ninh dữ liệu sau đây:

a) Thiết lập quy trình, quy định nội bộ về bảo vệ an ninh dữ liệu;

b) Áp dụng biện pháp, tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, mật mã, mã hóa, phân quyền truy cập, kiểm tra giám sát truy cập, sao lưu và khôi phục dữ liệu.

c) Có cơ chế kiểm soát chặt chẽ nhân sự trực tiếp tham gia xử lý dữ liệu chuyên ngành.

c) Kiểm tra, đánh giá rủi ro định kỳ đối với hệ thống, cơ sở, trung tâm lưu trữ dữ liệu chuyên ngành nhằm phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ đe dọa an ninh dữ liệu.

3. Trách nhiệm kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu:

a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu lưu trong hệ thống thông tin quan trọng quốc gia, các cơ sở, trung tâm dữ liệu chuyên ngành của cơ quan, tổ chức, doanh nghiệp nhà nước trừ trường hợp quy định tại điểm b và điểm c khoản này;

b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu lưu trong hệ thống thông tin quân sự, cơ sở, trung tâm dữ liệu thuộc Bộ Quốc phòng quản lý.

4. Chính phủ quy định chi tiết Điều này.

Chương V
TIÊU CHUẨN, QUY CHUẨN KỸ THUẬT AN NINH MẠNG

Điều 38. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng

1. Tiêu chuẩn an ninh mạng gồm tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn nước ngoài, tiêu chuẩn quốc gia và tiêu chuẩn cơ sở về an ninh mạng

đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng được công bố, thừa nhận áp dụng tại Việt Nam.

2. Quy chuẩn kỹ thuật an ninh mạng gồm quy chuẩn kỹ thuật quốc gia và quy chuẩn kỹ thuật địa phương về an ninh mạng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng được xây dựng, ban hành và áp dụng tại Việt Nam.

Điều 39. Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng

1. Chứng nhận hợp quy về an ninh mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng phù hợp với quy chuẩn kỹ thuật an ninh mạng.

2. Công bố hợp quy về an ninh mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng với quy chuẩn kỹ thuật an ninh mạng.

3. Chứng nhận hợp chuẩn về an ninh mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng phù hợp với tiêu chuẩn an ninh mạng.

4. Công bố hợp chuẩn về an ninh mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng với tiêu chuẩn an ninh mạng.

5. 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; thẩm định quy chuẩn kỹ thuật quốc gia về an ninh mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật.

6. Bộ Công an có trách nhiệm sau đây:

a) Xây dựng dự thảo tiêu chuẩn quốc gia về an ninh mạng, trừ tiêu chuẩn quốc gia quy định tại khoản 7 Điều này;

b) Xây dựng và ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng, trừ quy chuẩn quốc gia quy định tại khoản 7 Điều này;

c) Quản lý chất lượng sản phẩm, dịch vụ an ninh mạng;

d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng, trừ tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự.

7. Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng chủ trì, phối hợp Bộ Công an xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự.

8. Ủy ban nhân dân cấp tỉnh 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 an ninh mạng trên địa bàn.

Điều 40. 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 phải thực hiện chứng nhận hợp quy hoặc công bố hợp quy và sử dụng dấu hợp quy;

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

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

3. 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.

Chương VI
KINH DOANH SẢN PHẨM, DỊCH VỤ AN NINH MẠNG

Điều 41. Sản phẩm, dịch vụ an ninh mạng

1. Dịch vụ an ninh mạng gồm:

a) Dịch vụ kiểm tra, đánh giá an ninh mạng;

b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự;

c) Dịch vụ mật mã dân sự;

d) Dịch vụ tư vấn an ninh mạng;

đ) Dịch vụ giám sát an ninh mạng;

e) Dịch vụ ứng cứu sự cố an ninh mạng;

g) Dịch vụ khôi phục dữ liệu;

h) Dịch vụ phòng ngừa, chống tấn công mạng;

i) Dịch vụ an ninh mạng khác.

2. Sản phẩm an ninh mạng gồm:

a) Sản phẩm mật mã dân sự;

b) Sản phẩm kiểm tra, đánh giá an ninh mạng;

c) Sản phẩm giám sát an ninh mạng;

d) Sản phẩm chống tấn công, xâm nhập;

đ) Sản phẩm an ninh mạng khác.

3. Chính phủ quy định chi tiết danh mục sản phẩm, dịch vụ mật mã dân sự và các danh mục sản phẩm, dịch vụ an ninh mạng khác quy định tại khoản 1 và khoản 2 Điều này.

4. Chính phủ quy định chi tiết về việc kinh doanh sản phẩm, dịch vụ an ninh mạng.

Điều 42. Điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng

1. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng, trừ sản phẩm, dịch vụ quy định tại các điểm a, b, c và d khoản 1 và điểm a khoản 2 Điều 41 của Luật này, khi đáp ứng đủ các điều kiện sau đây:

a) Phù hợp với chiến lược, quy hoạch, kế hoạch phát triển an ninh mạng quốc gia;

b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ an ninh mạng;

c) Có nhân sự chịu trách nhiệm về bảo đảm an ninh mạng đáp ứng yêu cầu về kiến thức, kỹ năng về bảo đảm an ninh mạng, được cơ quan có thẩm quyền chứng nhận theo quy định;

d) Có phương án kinh doanh phù hợp;

đ) Có đăng ký ngành, nghề kinh doanh phù hợp;

e) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng được yêu cầu chuyên môn về an ninh mạng, nhân thân, lý lịch rõ ràng.

2. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ kiểm tra, đánh giá, giám sát an ninh mạng khi đáp ứng đủ các điều kiện sau đây:

a) Các điều kiện quy định tại khoản 1 Điều này;

b) Là doanh nghiệp được thành lập và hoạt động hợp pháp trên lãnh thổ Việt Nam, trừ doanh nghiệp có vốn đầu tư nước ngoài;

c) Người đại diện theo pháp luật, đội ngũ quản lý, điều hành, kỹ thuật là công dân Việt Nam thường trú tại Việt Nam;

d) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật;

đ) Có phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ;

e) Đội ngũ quản lý, điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về kiểm tra, đánh giá an ninh mạng.

3. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ bảo mật thông tin không sử dụng mật mã dân sự khi đáp ứng đủ các điều kiện sau đây:

a) Các điều kiện quy định tại các điểm a, b, c, d và đ khoản 2 Điều này;

b) Đội ngũ quản lý điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về bảo mật thông tin.

4. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ mật mã dân sự khi đáp ứng đủ các yêu cầu sau đây:

a) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng yêu cầu chuyên môn về bảo mật, an ninh mạng;

b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ mật mã dân sự;

c) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật;

d) Có phương án bảo mật và an ninh mạng trong quá trình quản lý và cung cấp sản phẩm, dịch vụ mật mã dân sự;

đ) Có phương án kinh doanh phù hợp;

e) Sản phẩm mật mã dân sự phải được kiểm định, chứng nhận hợp quy trước khi lưu thông trên thị trường.

5. Chính phủ quy định chi tiết về cấp, sửa đổi, bổ sung, cấp lại, gia hạn, tạm đình chỉ và thu hồi Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng.

Điều 43. Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng

1. Quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, báo cáo Bộ Công an về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng khi có yêu cầu.

2. Lập, lưu giữ và bảo mật thông tin của khách hàng.

3. Định kỳ hằng năm báo cáo Bộ Công an hoặc Ủy ban nhân dân tỉnh, thành phố về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng trước ngày 31 tháng 12.

4. Từ chối cung cấp sản phẩm, dịch vụ an ninh mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an ninh mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp.

5. Tạm ngừng hoặc ngừng cung cấp sản phẩm, dịch vụ an ninh mạng để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của cơ quan nhà nước có thẩm quyền.

6. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nghiệp vụ khi có yêu cầu.

Điều 44. Xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng

1. Việc quản lý xuất khẩu, nhập khẩu đối với sản phẩm an ninh mạng được thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan.

2. Việc xuất khẩu, nhập khẩu sản phẩm an ninh mạng của cơ quan, tổ chức, cá nhân được hưởng quyền ưu đãi, miễn trừ ngoại giao thực hiện theo quy định của pháp luật về hải quan, pháp luật về ưu đãi, miễn trừ dành cho cơ quan đại diện ngoại giao, cơ quan lãnh sự của nước ngoài và cơ quan đại diện của tổ chức quốc tế liên Chính phủ tại Việt Nam.

3. Trong trường hợp Việt Nam chưa có quy chuẩn kỹ thuật an ninh mạng tương ứng đối với sản phẩm an ninh mạng nhập khẩu thì áp dụng theo thỏa thuận quốc tế, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.

4. Chính phủ quy định chi tiết Điều này.

Chương VII
ĐIỀU KIỆN BẢO ĐẢM AN NINH MẠNG

Điều 45. Nghiên cứu, phát triển an ninh mạng

1. Nội dung nghiên cứu, phát triển an ninh mạng bao gồm:

a) Xây dựng hệ thống phần mềm, trang thiết bị bảo vệ an ninh mạng;

b) Phương pháp thẩm định phần mềm, trang thiết bị bảo vệ an ninh mạng đạt chuẩn và hạn chế tồn tại điểm yếu, lỗ hổng bảo mật, phần mềm độc hại;

c) Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng;

d) Phương pháp bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; khả năng bảo mật khi truyền đưa thông tin trên không gian mạng;

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

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

g) Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng;

h) Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng;

i) Dự báo an ninh mạng;

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

2. Cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.

Điều 46. Nâng cao năng lực tự chủ về an ninh mạng

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

2. Chính phủ thực hiện các biện pháp sau đây để nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân:

a) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng;

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

c) Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng;

d) Tăng cường môi trường kinh doanh, cải thiện điều kiện cạnh tranh hỗ trợ doanh nghiệp nghiên cứu, sản xuất sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng.

Điều 47. Lực lượng bảo vệ an ninh mạng

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

2. Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia.

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

Điều 48. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng

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

2. Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng.

3. Khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc nguy cơ đe dọa an ninh mạng, cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng.

Thẩm quyền, trách nhiệm, trình tự, thủ tục huy động nhân lực bảo vệ an ninh mạng được thực hiện theo quy định của Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và quy định khác của pháp luật có liên quan.

Điều 49. Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng

1. Công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng.

2. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao.

3. Ưu tiên phát triển cơ sở đào tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà nước và khu vực tư nhân, trong nước và nước ngoài.

Điều 50. Giáo dục bồi dưỡng kiến thức, nghiệp vụ an ninh mạng

1. Nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường, chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh.

2. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng.

Bộ Quốc phòng tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý.

Điều 51. Phổ biến kiến thức về an ninh mạng

1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng.

2. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức.

3. Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.

Điều 52. Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng

1. Lực lượng bảo vệ an ninh mạng quy định tại khoản 1 và khoản 2 Điều 47 Luật này phải đáp ứng yêu cầu kiến thức, kỹ năng về bảo đảm an ninh mạng.

2. Người trực tiếp quản trị, vận hành hệ thống thông tin cấp độ 3, 4 và 5 trong cơ quan, tổ chức, doanh nghiệp Nhà nước phải tham gia sát hạch và được cấp chứng chỉ kiến thức, kỹ năng về bảo đảm an ninh mạng.

3. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan tổ chức triển khai đánh giá, xác nhận đạt yêu cầu và cấp chứng chỉ kiến thức, kỹ năng về bảo đảm an ninh mạng thông qua chương trình bồi dưỡng, sát hạch và cấp chứng chỉ theo từng đối tượng liên quan.

4. Chính phủ quy định chi tiết chuẩn kiến thức, nội dung chương trình bồi dưỡng, thẩm quyền sát hạch, cấp chứng chỉ và lộ trình áp dụng đối với từng đối tượng liên quan

Điều 53. Kinh phí bảo vệ an ninh mạng

1. Kinh phí bảo vệ an ninh mạng của cơ quan nhà nước, tổ chức chính trị do ngân sách nhà nước bảo đảm, được bố trí trong dự toán ngân sách nhà nước hằng năm. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật về ngân sách nhà nước.

2. Kinh phí bảo vệ an ninh mạng của cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị phải bảo đảm tối thiểu 10% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin.

3. Kinh phí bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan, tổ chức ngoài quy định tại khoản 1 Điều này do cơ quan, tổ chức tự bảo đảm.

Điều 54. Quản lý nhà nước về an ninh mạng

1. Nội dung quản lý nhà nước về an ninh mạng bao gồm:

a) Xây dựng chủ trương, chính sách, chiến lược, quy hoạch, kế hoạch, chương trình trong lĩnh vực an ninh mạng.

b) Ban hành và tổ chức thực hiện văn bản quy phạm pháp luật về an ninh mạng; xây dựng, ban hành tiêu chuẩn quy chuẩn kỹ thuật an ninh mạng.

c) Quản lý hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng.

d) Quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy về an ninh mạng.

e) Quản lý công tác giám sát an ninh mạng.

g) Thẩm định về an ninh mạng trong hồ sơ thiết kế hệ thống thông tin.

h) Tuyên truyền, phổ biến pháp luật về an ninh mạng.

i) Tổ chức nghiên cứu, ứng dụng khoa học và công nghệ về an ninh mạng; phát triển nguồn nhân lực an ninh mạng; đào tạo về an ninh mạng.

k) Phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, tội

phạm sử dụng công nghệ cao.

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

m) Hợp tác quốc tế về an ninh mạng.

2. Trách nhiệm quản lý nhà nước về an ninh mạng

a) Chính phủ thống nhất quản lý nhà nước về an ninh mạng.

b) Bộ Công an là cơ quan đầu mối giúp Chính phủ thực hiện quản lý nhà nước về an ninh mạng, trừ quy định tại điểm c khoản này.

c) Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng thuộc phạm vi quản lý.

Ban Cơ yếu Chính phủ chịu trách nhiệm trước Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự và an ninh mạng thuộc phạm vi quản lý theo quy định của pháp luật về cơ yếu.

d) Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình thực hiện công tác bảo vệ an ninh mạng; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng;

e) Ủy ban nhân dân cấp tỉnh thực hiện công tác bảo vệ an ninh mạng và quản lý nhà nước về dữ liệu tại địa phương.

Chương VIII
TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN TRONG BẢO ĐẢM AN NINH MẠNG

Điều 55. Trách nhiệm của Bộ Công an

1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng;

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

3. Phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam quy định tại khoản 1 Điều 36 của Luật này.

4. Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về an ninh mạng trên dịch vụ, hệ thống thông tin do doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý.

5. 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;

6. Bảo đảm an ninh thông tin trên không gian mạng, an ninh dữ liệu; xây dựng cơ chế quản lý định danh IP; xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin an ninh mạng, nguy cơ đe dọa an ninh mạng;

7. Tham mưu, đề xuất Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều Bộ, ngành;

8. Tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

9. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng, an ninh thông tin, an ninh dữ liệu.

Điều 56. Trách nhiệm của Bộ Quốc phòng

1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý;

2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong phạm vi quản lý;

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

4. Phối hợp với Bộ Công an tổ chức diễn tập phòng, chống tấn công mạng, diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, triển khai thực hiện công tác bảo vệ an ninh mạng;

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

Điều 57. Trách nhiệm của Ban Cơ yếu Chính phủ

1. Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ an ninh mạng thuộc phạm vi Ban Cơ yếu Chính phủ quản lý.

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

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

Điều 58. Trách nhiệm của Bộ, ngành, Ủy ban nhân dân các cấp

Trong phạm vi nhiệm vụ, quyền hạn của mình, Bộ, ngành, Ủy ban nhân các cấp có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin thuộc phạm vi quản lý; phối hợp với lực lượng Công an nhân dân cấp tương ứng thực hiện quản lý nhà nước về an ninh mạng của Bộ, ngành, địa phương.

Điều 59. Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng

1. Chủ quản hệ thống thông tin có trách nhiệm thực hiện bảo vệ hệ thống thông tin theo quy định tại Luật này.

2. Kết nối hệ thống giám sát an ninh mạng, hệ thống phòng chống mã độc tập trung về Trung tâm An ninh mạng quốc gia của Bộ Công an hoặc Trung tâm An ninh mạng của tỉnh để hỗ trợ giám sát an ninh mạng.

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

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

a) Có phương án bảo đảm an ninh mạng được cơ quan nhà nước có thẩm quyền thẩm định khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin;

b) Chỉ định cá nhân, bộ phận phụ trách về an ninh mạng.

Điều 60. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng

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

2. Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa.

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

4. Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp 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 đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này;

5. Thực hiện theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh

mạng thuộc Bộ Công an để quản lý định danh IP.

6. Phối hợp, thực hiện theo yêu cầu, hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để thiết lập hệ thống kết nối, đấu nối đường truyền kỹ thuật, truyền tải dữ liệu và đáp ứng các điều kiện cần thiết khác để triển khai các giải pháp, biện pháp bảo vệ an ninh mạng.

7. Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm thực hiện quy định tại Điều này, khoản 2 và khoản 3 Điều 36 của Luật này.

Điều 61. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng

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

2. Có trách nhiệm bảo mật thông tin đăng ký, mở, quản lý, sử dụng tài khoản số của mình; trường hợp tài khoản số được sử dụng để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ vi phạm, chủ tài khoản bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường thiệt hại theo quy định pháp luật.

3. Cung cấp thông tin, tài liệu cho cơ quan có thẩm quyền, nhà cung cấp dịch vụ trung thực, đầy đủ theo quy định pháp luật.

4. Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng.

Chương IX
ĐIỀU KHOẢN THI HÀNH

Điều 62. Hiệu lực thi hành

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

2. Luật An toàn thông tin mạng số 86/2015/QH13 ban hành ngày 19 tháng 11 năm 2015 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 và Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018 hết hiệu lực kể từ ngày Luật này có hiệu lực thi hành, trừ trường hợp quy định tại Điều 63 của Luật này.

Điều 63. Điều khoản chuyển tiếp

1. Đối với các hồ sơ hệ thống thông tin đã có Quyết định công nhận cấp độ trước khi Luật này có hiệu lực thì không cần hoàn thiện hồ sơ theo quy định cấp độ mới, nhưng áp dụng các điều kiện, tiêu chuẩn, biện pháp bảo vệ tương

ướng với quy định cấp độ mới trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

2. Đối với hệ thống thông tin quan trọng quốc gia đã đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành:

a) Chủ quản hệ thống thông tin có trách nhiệm rà soát, đánh giá và thực hiện các biện pháp bảo đảm an ninh mạng theo quy định của Luật này;

b) Trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành, chủ quản hệ thống thông tin phải hoàn thành việc đánh giá điều kiện an ninh mạng và thẩm định an ninh mạng theo quy định của Luật này.

3. Các phương án, quy trình, thủ tục bảo đảm an toàn thông tin được ban hành theo Luật An toàn thông tin mạng số 86/2015/QH13 ban hành ngày 19 tháng 11 năm 2015 được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 phải được rà soát, điều chỉnh, bổ sung cho phù hợp với các quy định của Luật này trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

4. Các sản phẩm, dịch vụ, giải pháp, phương tiện kỹ thuật bảo đảm an toàn thông tin mạng đã được đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành, nếu không đáp ứng các điều kiện an ninh mạng theo quy định của Luật này thì phải được thay thế hoặc nâng cấp trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành.

5. Chính phủ quy định chi tiết Điều này.

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

CHỦ TỊCH QUỐC HỘI

Trần Thanh Mẫn

BỘ CÔNG AN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày tháng năm 2025

BẢN SO SÁNH DỰ THẢO LUẬT AN NINH MẠNG VỚI QUY ĐỊNH PHÁP LUẬT HIỆN HÀNH

STT	VĂN BẢN ĐƯỢC SỬA ĐỔI, BỔ SUNG, THAY THẾ 1 (LUẬT AN NINH MẠNG)	VĂN BẢN ĐƯỢC SỬA ĐỔI, BỔ SUNG, THAY THẾ 2 (LUẬT AN TOÀN THÔNG TIN MẠNG)	DỰ THẢO VĂN BẢN MỚI	THUYẾT MINH
1.1	Điều 1. Phạm vi điều chỉnh Luật này quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.	Điều 1. Phạm vi điều chỉnh Luật này quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng.	Điều 1. Phạm vi điều chỉnh Luật này quy định về hoạt động bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội và bảo vệ quyền, lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân trên không gian mạng; bảo đảm an ninh thông tin, an ninh dữ liệu, an toàn hệ thống thông tin; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.	- HỢP NHẤT LUẬT AN NINH MẠNG 2018 VÀ LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018). - BỔ SUNG THÊM MỚI 01 PHẠM VI ĐIỀU CHỈNH VỚI AN NINH DỮ LIỆU
2.2		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 đến hoạt động an toàn thông tin mạng tại Việt Nam.	Điều 2. Đối tượng áp dụng Luật này áp dụng đối với cơ quan, tổ chức, cá nhân Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam; cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng tại Việt Nam.	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018), ĐIỀU CHỈNH THÀNH TƯNG NHÓM ĐỐI TƯỢNG ÁP DỤNG

3.3	Điều 2. Giải thích từ ngữ Trong Luật này, các từ ngữ dưới đây được hiểu như sau: 1. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 2. *Bảo vệ an ninh mạng* là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng. 3. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. 4. *Không gian mạng quốc gia* là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát. 5. *Cơ sở hạ tầng không gian mạng quốc gia* là hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng quốc gia, bao gồm: a) Hệ thống truyền dẫn bao gồm	Điều 3. Giải thích từ ngữ Trong Luật này, các từ ngữ dưới đây được hiểu như sau: 1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. 2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính. 3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng. 4. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia. 5. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. 6. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống	Trong Luật này, các từ ngữ dưới đây được hiểu như sau: 1. An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; bảo đảm an ninh dữ liệu; bảo vệ thông tin, hệ thống thông tin, nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. 2. Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng. 3. Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính. 4. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. 5. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng.	- HỢP NHẤT LUẬT AN NINH MẠNG 2018 VÀ LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018). - BỔ SUNG MỚI 08 KHÁI NIỆM

	hệ thống truyền dẫn quốc gia, hệ thống truyền dẫn kết nối quốc tế, hệ thống vệ tinh, hệ thống truyền dẫn của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng; b) Hệ thống các dịch vụ lõi bao gồm hệ thống phân luồng và điều hướng thông tin quốc gia, hệ thống phân giải tên miền quốc gia (DNS), hệ thống chứng thực quốc gia (PKI/CA) và hệ thống cung cấp dịch vụ kết nối, truy cập Internet của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng; c) Dịch vụ, ứng dụng công nghệ thông tin bao gồm dịch vụ trực tuyến; ứng dụng công nghệ thông tin có kết nối mạng phục vụ quản lý, điều hành của cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng; cơ sở dữ liệu quốc gia. Dịch vụ trực tuyến bao gồm chính phủ điện tử, thương mại điện tử, trang thông tin điện tử, diễn đàn trực tuyến, mạng xã hội, blog; d) Cơ sở hạ tầng công nghệ	thông tin. 7. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng. 8. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng. 9. *Đánh giá rủi ro an toàn thông tin mạng* là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin. 10. *Quản lý rủi ro an toàn thông tin mạng* là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng. 11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin. 12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại. 13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử,	6. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. 7. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin. 8. Phần cứng độc hại là các bộ phận vật lý của hệ thống máy tính, hệ thống thông tin, được tạo ra có chủ đích, nằm ngoài thiết kế và quy cách thiết bị tiêu chuẩn, có thể được điều khiển hoặc thực hiện tính năng can thiệp vào phần mềm, phần cứng hệ thống, gây ra tác động bất bình thường cho một phần hay toàn bộ hệ thống máy tính, hệ thống thông tin, hoặc đánh cắp thông tin, dữ liệu trái phép lưu trữ trong hệ thống máy tính, hệ thống thông tin, hoặc gây ngừng trệ, tê liệt, phá hoại hệ thống tùy theo mục đích thiết kế. 9. Nhật ký hệ thống là hệ thống được thiết lập có chức năng ghi nhận, lưu trữ và có thể trích xuất dữ liệu phản ánh những sự kiện liên quan đến trạng thái hoạt động, sự cố, sự kiện an ninh mạng của hệ thống và dữ liệu do người dùng tạo ra trong quá trình sử dụng hệ thống, truy cập dịch vụ Internet. 10. Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin	

	thông tin của đô thị thông minh, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh và hệ thống trí tuệ nhân tạo. 6. *Cổng kết nối mạng quốc tế* là nơi diễn ra hoạt động chuyển nhận tín hiệu mạng qua lại giữa Việt Nam và các quốc gia, vùng lãnh thổ khác. 7. *Tội phạm mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự. 8. *Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử. 9. *Khủng bố mạng* là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố. 10. *Gián điệp mạng* là hành vi cố ý vượt qua cảnh báo, mã truy	số điện thoại, địa chỉ Internet và hình thức tương tự khác. 14. *Xung đột thông tin* là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng. 15. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể. 16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó. 17. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại. 18. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước. 19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin. 20. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.	hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự. 11. Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử. 12. Khủng bố mạng là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố. 13. Gián điệp mạng là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác nhằm chiếm đoạt, thu thập trái phép tài liệu, thông tin bí mật, tài nguyên thông tin của cơ quan, tổ chức Nhà nước hoặc nhằm mục đích gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội. 14. Nguy cơ đe dọa an ninh mạng là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 15. Sự cố an ninh mạng là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn	

	cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của cơ quan, tổ chức, cá nhân. 11. *Tài khoản số* là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng. 12. *Nguy cơ đe dọa an ninh mạng* là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 13. *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 14. *Tình huống nguy hiểm về an ninh mạng* là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh		xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 16. Xung đột thông tin là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng. 17. Tình huống nguy hiểm về an ninh mạng là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 18. Tài khoản số là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng. 19. Mật mã dân sự là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước. 20. Sản phẩm an ninh mạng là phần cứng, phần mềm có chức năng bảo vệ an ninh mạng, an ninh thông tin, an ninh dữ liệu, thông tin, hệ thống thông tin, cơ sở hạ tầng công nghệ thông tin. 21. Dịch vụ an ninh mạng là dịch vụ được cung cấp để bảo vệ an ninh mạng, an ninh thông tin, an ninh dữ liệu, thông tin, hệ thống thông tin, cơ sở hạ tầng công nghệ thông tin.	

	quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.			
4.4	Điều 3. Chính sách của Nhà nước về an ninh mạng 1. Ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại. 2. Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 3. Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng. 4. Khuyến khích, tạo điều kiện	Điều 5. Chính sách của Nhà nước về an toàn thông tin mạng 1. Đẩy mạnh đào tạo, phát triển nguồn nhân lực và xây dựng cơ sở hạ tầng, kỹ thuật an toàn thông tin mạng đáp ứng yêu cầu ổn định chính trị, phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội. 2. Khuyến khích nghiên cứu, phát triển, áp dụng biện pháp kỹ thuật, công nghệ, hỗ trợ xuất khẩu, mở rộng thị trường cho sản phẩm, dịch vụ an toàn thông tin mạng do tổ chức, cá nhân trong nước sản xuất, cung cấp; tạo điều kiện nhập khẩu sản phẩm, công nghệ hiện đại mà tổ chức, cá nhân trong nước chưa có năng lực sản xuất, cung cấp. 3. Bảo đảm môi trường cạnh tranh lành mạnh trong hoạt động kinh doanh sản phẩm, dịch vụ an toàn	Điều 4. Chính sách của Nhà nước về an ninh mạng 1. Ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại. 2. Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 3. Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng, bảo đảm nguồn nhân lực trình độ cao cho bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng; có cơ chế đặc thù, chính sách ưu đãi để huy động, thu hút và sử dụng nhân tài	- HỢP NHẤT LUẬT AN NINH MẠNG 2018 VÀ LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018). - BỔ SUNG MỚI 01 CHÍNH SÁCH

	để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng. 5. Tăng cường hợp tác quốc tế về an ninh mạng.	thông tin mạng; khuyến khích, tạo điều kiện cho tổ chức, cá nhân tham gia đầu tư, nghiên cứu, phát triển và cung cấp sản phẩm, dịch vụ an toàn thông tin mạng. 4. Nhà nước bố trí kinh phí để bảo đảm an toàn thông tin mạng của cơ quan nhà nước và an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.	trong lĩnh vực an ninh mạng.. 4. Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng. 5. Tăng cường hợp tác quốc tế về an ninh mạng.	
5.5	Điều 4. Nguyên tắc bảo vệ an ninh mạng 1. Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng. 3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.	Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng 1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội. 2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác. 3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức. 4. Hoạt động an toàn thông tin mạng	Điều 5. Nguyên tắc bảo vệ an ninh mạng 1. Tuân thủ Hiến pháp và pháp luật; bảo đảm an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng. 2. Đặt dưới sự lãnh đạo tuyệt đối, trực tiếp của Đảng Cộng sản Việt Nam; sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng. 3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng quốc gia, bảo vệ an ninh dữ liệu với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng. 4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại hoạt động sử dụng không gian mạng xâm	- HỢP NHẤT LUẬT AN NINH MẠNG 2018 VÀ LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018). - BỔ SUNG MỚI 01 NGUYÊN TẮC

	4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng. 5. Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia. 6. Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng. 7. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.	phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.	phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 5. Triển khai hoạt động bảo vệ an ninh mạng thường xuyên, liên tục đối với cơ sở hạ tầng không gian mạng quốc gia nhằm bảo vệ vững chắc nền tảng của công cuộc chuyển đổi số quốc gia, hướng đến mục tiêu tự chủ về công nghệ an ninh mạng, ưu tiên trong những lĩnh vực chiến lược. 6. Chủ động áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng quốc gia; bảo đảm hệ thống thông tin quan trọng quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng. 7. Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng. 8. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.	
6.6.	Điều 5. Biện pháp bảo vệ an ninh mạng		Điều 6. Biện pháp bảo vệ an ninh mạng	- KẾ THỪA LUẬT AN NINH MẠNG NĂM

	1. Biện pháp bảo vệ an ninh mạng bao gồm: a) Thẩm định an ninh mạng; b) Đánh giá điều kiện an ninh mạng; c) Kiểm tra an ninh mạng; d) Giám sát an ninh mạng; đ) Ứng phó, khắc phục sự cố an ninh mạng; e) Đấu tranh bảo vệ an ninh mạng; g) Sử dụng mật mã để bảo vệ thông tin mạng; h) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; i) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; k) Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá		1. Biện pháp bảo vệ an ninh mạng bao gồm: a) Thẩm định an ninh mạng; b) Đánh giá điều kiện an ninh mạng; c) Kiểm tra an ninh mạng; d) Giám sát an ninh mạng; đ) Ứng phó, khắc phục sự cố an ninh mạng; e) Đấu tranh bảo vệ an ninh mạng; g) Sử dụng mật mã để bảo vệ thông tin mạng; h) Sử dụng giải pháp kỹ thuật để bảo vệ dữ liệu; bảo vệ thông tin, hệ thống thông tin; ngăn chặn thông tin vi phạm pháp luật. i) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; k) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; l) Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng; m) Phong tỏa, hạn chế hoạt động của	2018

	nhân trên không gian mạng; l) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật; m) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự; n) Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính. 2. Chính phủ quy định trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm m và điểm n khoản 1 Điều này.		hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật; n) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự; p) Biện pháp khác theo quy định của pháp luật về bảo vệ an ninh quốc gia, pháp luật về xử lý vi phạm hành chính. 2. Chính phủ quy định chi tiết về nội dung, trình tự, thủ tục, thẩm quyền áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm n và điểm o khoản 1 Điều này.	
7.7.	Điều 6. Bảo vệ không gian mạng quốc gia Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.		Điều 7. Bảo vệ không gian mạng quốc gia Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018
8.8.	Điều 7. Hợp tác quốc tế về an ninh mạng 1. Hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền	Điều 6. Hợp tác quốc tế về an toàn thông tin mạng 1. Hợp tác quốc tế về an toàn thông tin mạng phải tuân thủ các nguyên tắc sau đây:	Điều 8. Hợp tác quốc tế về an ninh mạng 1. Hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền, toàn vẹn lãnh thổ,	- HỢP NHẤT LUẬT AN NINH MẠNG 2018 VÀ LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015

	và toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi. 2. Nội dung hợp tác quốc tế về an ninh mạng bao gồm: a) Nghiên cứu, phân tích xu hướng an ninh mạng; b) Xây dựng cơ chế, chính sách nhằm đẩy mạnh hợp tác giữa tổ chức, cá nhân Việt Nam với tổ chức, cá nhân nước ngoài, tổ chức quốc tế hoạt động về an ninh mạng; c) Chia sẻ thông tin, kinh nghiệm; hỗ trợ đào tạo, trang thiết bị, công nghệ bảo vệ an ninh mạng; d) Phòng, chống tội phạm mạng, hành vi xâm phạm an ninh mạng; ngăn ngừa các nguy cơ đe dọa an ninh mạng; đ) Tư vấn, đào tạo và phát triển nguồn nhân lực an ninh mạng; e) Tổ chức hội nghị, hội thảo và diễn đàn quốc tế về an ninh mạng; g) Ký kết và thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng; h) Thực hiện chương trình, dự án hợp tác quốc tế về an ninh mạng; i) Hoạt động hợp tác quốc tế khác về an ninh mạng.	a) Tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ quốc gia, không can thiệp vào công việc nội bộ của nhau, bình đẳng và các bên cùng có lợi; b) Phù hợp với quy định của pháp luật Việt Nam, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên. 2. Nội dung hợp tác quốc tế về an toàn thông tin mạng gồm: a) Hợp tác quốc tế trong đào tạo, nghiên cứu và ứng dụng khoa học, kỹ thuật, công nghệ về an toàn thông tin mạng; b) Hợp tác quốc tế trong phòng, chống hành vi vi phạm pháp luật về an toàn thông tin mạng; điều tra, xử lý sự cố an toàn thông tin mạng, ngăn chặn hoạt động lợi dụng mạng để khủng bố; c) Hoạt động hợp tác quốc tế khác về an toàn thông tin mạng.	không can thiệp vào công việc nội bộ của nhau, bình đẳng, cùng có lợi và tuân thủ Hiến pháp, pháp luật Việt Nam, điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên. 2. Nội dung hợp tác quốc tế về an ninh mạng bao gồm: a) Chia sẻ thông tin, dữ liệu và cảnh báo sớm về nguy cơ, sự cố, tấn công mạng ảnh hưởng đến an ninh mạng; b) Xây dựng khuôn khổ pháp lý, chính sách và cơ chế phối hợp trong bảo vệ an ninh mạng; ký kết, tham gia thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng; c) Đào tạo, tư vấn, chia sẻ kinh nghiệm và nâng cao năng lực chuyên môn, kỹ thuật trong lĩnh vực an ninh mạng; d) Phòng, chống tội phạm sử dụng công nghệ cao; phối hợp điều tra, xử lý vi phạm pháp luật và tội phạm sử dụng công nghệ cao có yếu tố nước ngoài; đ) Nghiên cứu, phát triển, chuyển giao công nghệ, sản phẩm, giải pháp kỹ thuật phục vụ công tác bảo vệ an ninh mạng; e) Tổ chức hội nghị, hội thảo, diễn đàn quốc tế và triển khai các chương trình, dự án hợp tác quốc tế về an ninh mạng; g) Hoạt động hợp tác quốc tế khác về an ninh mạng. 3. Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện	(SỬA ĐỔI, BỔ SUNG NĂM 2018). - BỔ SUNG MỚI 05 NỘI DUNG HỢP TÁC QUỐC TẾ

	3. Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng. Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vi quản lý. Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng. Trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều Bộ, ngành do Chính phủ quyết định. 4. Hoạt động hợp tác quốc tế về an ninh mạng của Bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.		hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng. Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vi quản lý. Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng. Trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều Bộ, ngành do Chính phủ quyết định. 4. Hoạt động hợp tác quốc tế về an ninh mạng của Bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.	
9.8.	Điều 8. Các hành vi bị nghiêm cấm về an ninh mạng 1. Sử dụng không gian mạng để thực hiện hành vi sau đây: a) Hành vi quy định tại khoản 1 Điều 18 của Luật này; b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người	Điều 7. Các hành vi bị nghiêm cấm 1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật. 2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng	Điều 9. Các hành vi bị nghiêm cấm về an ninh mạng 1. Sử dụng không gian mạng để đăng tải, phát tán thông tin có nội dung: a) Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược,	- HỢP NHẤT LUẬT AN NINH MẠNG 2018 VÀ LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018). - LIỆT KÊ ĐẦY ĐỦ CÁC HÀNH VI LUẬT

	chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; e) Xúi giục, lôi kéo, kích động người khác phạm tội. 2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia. 3. Sản xuất, đưa vào sử dụng	truy nhập hệ thống thông tin của người sử dụng. 3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin. 4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo. 5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân. 6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.	chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc; b) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; c) Bịa đặt, vu khống, vu cáo sai sự thật, xúc phạm danh dự, uy tín, nhân phẩm của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; d) Sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán. 2. Sử dụng không gian mạng để thực hiện hành vi sau đây: a) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào	AN NINH MẠNG 2018 QUY ĐỊNH DẪN CHIẾU

	công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác. 4. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng. 5. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi. 6. Hành vi khác vi phạm quy định của Luật này.		tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; b) Kích động, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự; c) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật Nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc; d) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; đ) Lừa đảo chiếm đoạt tài sản; tổ chức	

			đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng; e) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức Nhà nước; f) Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác; g) Hướng dẫn, xúi giục, lôi kéo, kích động người khác phạm tội hoặc thực hiện hành vi vi phạm pháp luật; h) Thực hiện hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội. 3. Thực hiện tấn công mạng; khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin	

			4. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác. 5. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng. 6. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi. 7. Hành vi khác vi phạm quy định của Luật này.	
10.9	Điều 9. Xử lý vi phạm pháp luật về an ninh mạng Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm	Điều 8. Xử lý vi phạm pháp luật về an toàn thông tin mạng Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ	Điều 10. Xử lý vi phạm pháp luật về an ninh mạng Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.	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.	luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.	
11.10		Điều 21. Phân loại cấp độ an toàn hệ thống thông tin 1. Phân loại cấp độ an toàn hệ thống thông tin là việc xác định cấp độ an toàn thông tin của hệ thống thông tin theo cấp độ tăng dần từ 1 đến 5 để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ. 2. Hệ thống thông tin được phân loại theo cấp độ an toàn như sau: a) Cấp độ 1 là cấp độ mà khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia; b) Cấp độ 2 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia; c) Cấp độ 3 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;	Điều 11. Phân loại cấp độ hệ thống thông tin 1. Phân loại cấp độ hệ thống thông tin là việc xác định cấp độ an ninh mạng của hệ thống thông tin để áp dụng biện pháp bảo vệ tương ứng, phù hợp theo từng cấp độ tăng dần từ 1 đến 5. 2. Hệ thống thông tin được phân loại theo cấp độ như sau: a) Cấp độ 1 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia; b) Cấp độ 2 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia; c) Cấp độ 3 là cấp độ mà khi bị sự cố,	KẾ THỪA 5 CẤP ĐỘ THEO QUY ĐỊNH TẠI LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018), ĐIỀU CHỈNH THEO CÔNG TÁC CỦA CÔNG AN

		d) Cấp độ 4 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia; đ) Cấp độ 5 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia. 3. Chính phủ quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ.	xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia; d) Cấp độ 4 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia; đ) Cấp độ 5 là cấp độ mà khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới chủ quyền, lợi ích, quốc phòng, an ninh quốc gia. 3. Chính phủ quy định chi tiết tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin; các biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin và trách nhiệm, nghĩa vụ bảo đảm an ninh mạng theo từng cấp độ của hệ thống thông tin.	
12.		Điều 22. Nhiệm vụ bảo vệ hệ thống thông tin 1. Xác định cấp độ an toàn thông tin của hệ thống thông tin. 2. Đánh giá và quản lý rủi ro an toàn	Điều 12. Nhiệm vụ bảo vệ hệ thống thông tin 1. Nội dung nhiệm vụ bảo vệ hệ thống thông tin, bao gồm: a) Xác định cấp độ an ninh mạng của	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		hệ thống thông tin. 3. Đôn đốc, giám sát, kiểm tra công tác bảo vệ hệ thống thông tin. 4. Tổ chức triển khai các biện pháp bảo vệ hệ thống thông tin. 5. Thực hiện chế độ báo cáo theo quy định. 6. Tổ chức tuyên truyền, nâng cao nhận thức về an toàn thông tin mạng.	hệ thống thông tin và hệ thống thông tin quan trọng quốc gia. b) Đánh giá và quản lý rủi ro an ninh mạng hệ thống thông tin. c) Đôn đốc, giám sát, kiểm tra công tác bảo vệ an ninh mạng hệ thống thông tin. d) Tổ chức triển khai các biện pháp bảo vệ an ninh mạng hệ thống thông tin. e) Thực hiện chế độ báo cáo theo quy định. g) Tổ chức tuyên truyền, nâng cao nhận thức về an ninh mạng. 2. Chủ quản hệ thống thông tin thuộc Cấp độ 1 và Cấp độ 2 tự chịu trách nhiệm thực hiện các nội dung quy định tại Khoản 1 Điều này. 3. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4, Cấp độ 5 phải thực hiện đầy đủ các nội dung nhiệm vụ quy định tại Khoản 1 Điều này.	
13.		Điều 23. Biện pháp bảo vệ hệ thống thông tin 1. Ban hành quy định về bảo đảm an toàn thông tin mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin. 2. Áp dụng biện pháp quản lý, kỹ thuật theo tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng để phòng, chống nguy cơ, khắc phục sự cố an toàn thông tin mạng.	Điều 13. Biện pháp bảo vệ hệ thống thông tin 1. Các biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin, bao gồm: a) Ban hành quy định về bảo đảm an ninh mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp, hủy bỏ hệ thống thông tin. b) Thẩm định an ninh mạng đối với hồ sơ, thiết kế của hệ thống thông tin. c) Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin.	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		3. Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng. 4. Giám sát an toàn hệ thống thông tin.	d) Áp dụng biện pháp quản lý theo tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng, nghiên cứu xây dựng hệ thống tường lửa quốc gia để phòng, chống nguy cơ, khắc phục sự cố an ninh mạng. đ) Kiểm tra, giám sát việc tuân thủ quy định và đánh giá hiệu quả của các biện pháp quản lý và kỹ thuật được áp dụng. e) Thực hiện giám sát an ninh mạng. g) Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin 2. Chủ quản hệ thống thông tin thuộc Cấp độ 1 và Cấp độ 2 có thể lựa chọn áp dụng đầy đủ hoặc một số biện pháp quy định tại Khoản 1 Điều này tùy theo nhu cầu và khả năng đáp ứng thực tế. 3. Chủ quản hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4, Cấp độ 5 phải áp dụng đầy đủ các biện pháp quy định tại Khoản 1 Điều này. 4. Chính phủ quy định chi tiết về nội dung nhiệm vụ và biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ và đối với hệ thống thông tin quan trọng về an ninh quốc gia, được quy định tại khoản 1 Điều 12 và khoản 1 Điều 13 Luật này.	
14.	**Điều 10. Hệ thống thông tin quan trọng về an ninh quốc gia** 1. Hệ thống thông tin quan		Điều 14. Hệ thống thông tin quan trọng về an ninh quốc gia 1. Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018, BỔ SUNG THÊM NỘI DUNG

	trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng. 2. Hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; b) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; c) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng; d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái; đ) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; e) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương; g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông,		thuộc Cấp độ 5; hoặc hệ thống thông tin thuộc Cấp độ 3, Cấp độ 4 và đáp ứng một số tiêu chí nhất định theo quy định của Chính phủ. 2. Danh mục hệ thống thông tin quan trọng về an ninh quốc gia là danh sách hệ thống thông tin quan trọng về an ninh quốc gia được xác lập, ban hành và áp dụng biện pháp bảo vệ tương xứng nhằm bảo đảm hoạt động ổn định của các lĩnh vực quan trọng, bao gồm: a) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; b) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; c) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng; d) Hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái; đ) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; e) Hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở trung ương; g) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí;	LIÊN QUAN ĐẾN LUẬT AN TOÀN THÔNG TIN MẠNG

	giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí; h) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia. 3. Thủ tướng Chính phủ ban hành và sửa đổi, bổ sung Danh mục hệ thống thông tin quan trọng về an ninh quốc gia. 4. Chính phủ quy định việc phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, các Bộ, ngành chức năng trong việc thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia.		h) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia. 3. Thủ tướng Chính phủ ban hành và sửa đổi, bổ sung Danh mục hệ thống thông tin quan trọng quốc gia. Bộ Công an chủ trì, phối hợp bộ, ngành có liên quan xây dựng Danh mục hệ thống thông tin quan trọng quốc gia trình Thủ tướng Chính phủ ban hành, sửa đổi, bổ sung.	
15.	**Điều 11. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia** 1. Thẩm định an ninh mạng là hoạt động xem xét, đánh giá những nội dung về an ninh mạng để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin. 2. Đối tượng thẩm định an ninh mạng đối với hệ thống thông tin		Điều 15. Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 1. Thẩm định an ninh mạng là hoạt động xem xét, đánh giá những nội dung về an ninh mạng để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin. 2. Đối tượng thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Báo cáo nghiên cứu tiền khả thi, hồ	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	quan trọng về an ninh quốc gia bao gồm: a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt; b) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt. 3. Nội dung thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế; b) Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng. 4. Thẩm quyền thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân		sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt; b) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt. 3. Nội dung thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế; b) Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng. 4. Thẩm quyền thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.	

	sự; c) Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.			
16.	**Điều 12. Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia** 1. Đánh giá điều kiện về an ninh mạng là hoạt động xem xét sự đáp ứng về an ninh mạng của hệ thống thông tin trước khi đưa vào vận hành, sử dụng. 2. Hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng các điều kiện sau đây về: a) Quy định, quy trình và phương án bảo đảm an ninh mạng; nhân sự vận hành, quản trị hệ thống; b) Bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống; c) Biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng; biện pháp bảo vệ hệ thống điều khiển và giám sát tự động, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh, hệ thống trí tuệ nhân tạo;		Điều 16. Đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 1. Đánh giá điều kiện về an ninh mạng là hoạt động xem xét sự đáp ứng về an ninh mạng của hệ thống thông tin trước khi đưa vào vận hành, sử dụng. 2. Hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng các điều kiện sau đây về: a) Quy định, quy trình và phương án bảo đảm an ninh mạng; nhân sự vận hành, quản trị hệ thống; b) Bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống; c) Biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng; biện pháp bảo vệ hệ thống điều khiển và giám sát tự động, Internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh, hệ thống trí tuệ nhân tạo; d) Biện pháp bảo đảm an ninh vật lý bao gồm cách ly cô lập đặc biệt, chống rò rỉ dữ liệu, chống thu tin, kiểm soát ra vào. 3. Thẩm quyền đánh giá điều kiện an ninh mạng đối với hệ thống thông tin	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	d) Biện pháp bảo đảm an ninh vật lý bao gồm cách ly cô lập đặc biệt, chống rò rỉ dữ liệu, chống thu tin, kiểm soát ra vào. 3. Thẩm quyền đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ. 4. Hệ thống thông tin quan trọng về an ninh quốc gia được đưa vào vận hành, sử dụng sau khi được chứng nhận đủ điều kiện an ninh mạng. 5. Chính phủ quy định chi tiết khoản 2 Điều này.		quan trọng về an ninh quốc gia được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ. 4. Hệ thống thông tin quan trọng về an ninh quốc gia được đưa vào vận hành, sử dụng sau khi được chứng nhận đủ điều kiện an ninh mạng. 5. Chính phủ quy định chi tiết khoản 2 Điều này.	

17.	**Điều 13. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia** 1. Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin. 2. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện trong trường hợp sau đây: a) Khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin; b) Khi có thay đổi hiện trạng hệ thống thông tin; c) Kiểm tra định kỳ hằng năm; d) Kiểm tra đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; khi có yêu cầu quản lý nhà nước về an ninh mạng; khi hết thời hạn khắc phục điểm yếu, lỗ hổng		Điều 17. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 1. Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin. 2. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện trong trường hợp sau đây: a) Khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin; b) Khi có thay đổi hiện trạng hệ thống thông tin; c) Kiểm tra định kỳ hằng năm; d) Kiểm tra đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; khi có yêu cầu quản lý nhà nước về an ninh mạng; khi hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng. 3. Đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Hệ thống phần cứng, phần mềm,	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng. 3. Đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; b) Quy định, biện pháp bảo vệ an ninh mạng; c) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; d) Phương án ứng phó, khắc phục sự cố an ninh mạng của chủ quản hệ thống thông tin; đ) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật; e) Nhân lực bảo vệ an ninh mạng. 4. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý trong trường hợp quy định tại các điểm a, b và c khoản 2 Điều này; thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên		thiết bị số được sử dụng trong hệ thống thông tin; b) Quy định, biện pháp bảo vệ an ninh mạng; c) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; d) Phương án ứng phó, khắc phục sự cố an ninh mạng của chủ quản hệ thống thông tin; đ) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật; e) Nhân lực bảo vệ an ninh mạng. 4. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý trong trường hợp quy định tại các điểm a, b và c khoản 2 Điều này; thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đối với hệ thống thông tin quân sự. 5. Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông	

	trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đối với hệ thống thông tin quân sự. 5. Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; ít nhất là 72 giờ trong trường hợp có yêu cầu quản lý nhà nước về an ninh mạng hoặc hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng; b) Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục		tin ít nhất là 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; ít nhất là 72 giờ trong trường hợp có yêu cầu quản lý nhà nước về an ninh mạng hoặc hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng; b) Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin; c) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quân sự. Ban Cơ yếu Chính phủ kiểm tra an ninh mạng đột xuất đối với hệ thống	

	khi có đề nghị của chủ quản hệ thống thông tin; c) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quân sự. Ban Cơ yếu Chính phủ kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước; d) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất. 6. Kết quả kiểm tra an ninh mạng được bảo mật theo quy		thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước; d) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất. 6. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật.	

	định của pháp luật.			
18.	**Điều 14. Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia** 1. Giám sát an ninh mạng là hoạt động thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý. 2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp. 3. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý; cảnh báo và phối hợp		Điều 18. Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 1. Giám sát an ninh mạng là hoạt động thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý. 2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp. 3. Lực lượng chuyên trách bảo vệ an ninh mạng thực hiện giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia.			
19.		Điều 27. Trách nhiệm bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia 1. Chủ quản hệ thống thông tin quan trọng quốc gia có trách nhiệm sau đây: a) Thực hiện quy định tại khoản 2 Điều 25 của Luật này; b) Định kỳ đánh giá rủi ro an toàn thông tin mạng. Việc đánh giá rủi ro an toàn thông tin mạng phải do tổ chức chuyên môn được cơ quan nhà nước có thẩm quyền chỉ định thực hiện; c) Triển khai biện pháp dự phòng cho hệ thống thông tin; d) Lập kế hoạch bảo vệ, lập phương án và diễn tập phương án bảo vệ hệ thống thông tin quan trọng quốc gia. 2. Bộ Thông tin và Truyền thông có trách nhiệm sau đây: a) Chủ trì, phối hợp với chủ quản hệ thống thông tin quan trọng quốc gia, Bộ Công an và bộ, ngành có liên quan hướng dẫn, đôn đốc, thanh tra, kiểm tra công tác bảo vệ an toàn	Điều 19. Trách nhiệm bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 1. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm sau đây: a) Thực hiện quy định tại khoản 1 Điều 12 và khoản 1 Điều 13 Luật này; b) Khi thiết lập, mở rộng và nâng cấp hệ thống thông tin quan trọng về a ninh quốc gia phải thực hiện kiểm định an ninh mạng trước khi đi vào vận hành, khai thác; định kỳ hằng năm, tự kiểm tra, đánh giá an ninh mạng hệ thống thông tin quan trọng về an ninh quốc gia; và thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền; c) Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền trong việc thường xuyên thực hiện giám sát an ninh mạng; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng; đề ra phương án ứng phó, khắc	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		thông tin mạng đối với hệ thống thông tin quan trọng quốc gia, trừ hệ thống thông tin quy định tại khoản 3 và khoản 4 Điều này; b) Yêu cầu doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng tham gia tư vấn, hỗ trợ kỹ thuật, ứng cứu sự cố an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia. 3. Bộ Công an chủ trì hướng dẫn, đôn đốc, thanh tra, kiểm tra công tác bảo vệ an toàn thông tin mạng đối với hệ thống thông tin quan trọng quốc gia do Bộ Công an quản lý; phối hợp với Bộ Thông tin và Truyền thông, chủ quản hệ thống thông tin quan trọng quốc gia, bộ, ngành, Ủy ban nhân dân các cấp có liên quan trong việc bảo vệ hệ thống thông tin quan trọng quốc gia khác khi có yêu cầu của cơ quan nhà nước có thẩm quyền. 4. Bộ Quốc phòng chủ trì hướng dẫn, đôn đốc, thanh tra, kiểm tra công tác bảo vệ an toàn thông tin mạng đối với hệ thống thông tin quan trọng quốc gia do Bộ Quốc phòng quản lý. 5. Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã để bảo vệ thông tin trong hệ	phục khẩn cấp; d) Xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền; đ) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong việc thực hiện kiểm tra an ninh mạng đột xuất. 2. Bộ Công an có trách nhiệm sau đây đối với các hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu do Bộ Quốc phòng và Ban Cơ yếu Chính phủ quản lý theo quy định của pháp luật: a) Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; b) Đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; c) Kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia; d) Thực hiện giám sát an ninh mạng; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; đ) Chủ trì điều phối hoạt động ứng	

		thống thông tin quan trọng quốc gia của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội; phối hợp với chủ quản hệ thống thông tin quan trọng quốc gia trong việc giám sát an toàn thông tin mạng theo quy định của pháp luật.	phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia, tham gia ứng phó, khắc phục sự cố khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng; e) Chủ trì, phối hợp Ban Cơ yếu Chính phủ trong triển khai các biện bảo bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia có sử dụng giải pháp, sản phẩm mật mã của ngành Cơ yếu Việt Nam để bảo vệ bí mật nhà nước. 3. Bộ Quốc phòng chủ trì thẩm định, đánh giá, kiểm tra an ninh mạng đột xuất và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia do Bộ Quốc phòng quản lý. 4. Ban Cơ yếu Chính phủ chủ trì tổ chức triển khai giải pháp dùng mật mã để bảo vệ thông tin bí mật nhà nước trong hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định, đánh giá, kiểm tra an ninh mạng đột xuất, giám sát an ninh mạng và điều phối hoạt động ứng phó khắc phục sự cố an ninh mạng đối với hệ thống thông tin cơ yếu do Ban Cơ yếu Chính phủ quản lý.	
20.	Điều 15. Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia		Điều 20. Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia 1. Hoạt động ứng phó, khắc phục sự cố	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	1. Hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Phát hiện, xác định sự cố an ninh mạng; b) Bảo vệ hiện trường, thu thập chứng cứ; c) Phong tỏa, giới hạn phạm vi xảy ra sự cố an ninh mạng, hạn chế thiệt hại do sự cố an ninh mạng gây ra; d) Xác định mục tiêu, đối tượng, phạm vi cần ứng cứu; đ) Xác minh, phân tích, đánh giá, phân loại sự cố an ninh mạng; e) Triển khai phương án ứng phó, khắc phục sự cố an ninh mạng; g) Xác minh nguyên nhân và truy tìm nguồn gốc; h) Điều tra, xử lý theo quy định của pháp luật. 2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an		an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Phát hiện, xác định sự cố an ninh mạng; b) Bảo vệ hiện trường, thu thập chứng cứ; c) Phong tỏa, giới hạn phạm vi xảy ra sự cố an ninh mạng, hạn chế thiệt hại do sự cố an ninh mạng gây ra; d) Xác định mục tiêu, đối tượng, phạm vi cần ứng cứu; đ) Xác minh, phân tích, đánh giá, phân loại sự cố an ninh mạng; e) Triển khai phương án ứng phó, khắc phục sự cố an ninh mạng; g) Xác minh nguyên nhân và truy tìm nguồn gốc; h) Điều tra, xử lý theo quy định của pháp luật. 2. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền. 3. Điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Lực lượng chuyên trách bảo vệ an	

	ninh mạng có thẩm quyền. 3. Điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; tham gia ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.		ninh mạng thuộc Bộ Công an chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản này; tham gia ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ. 4. Cơ quan, tổ chức, cá nhân có trách nhiệm tham gia ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu của lực lượng chủ trì điều phối.	

	4. Cơ quan, tổ chức, cá nhân có trách nhiệm tham gia ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu của lực lượng chủ trì điều phối.			
21.	Điều 24. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia 1. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trong trường hợp sau đây: a) Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội; b) Khi có đề nghị của chủ quản hệ thống thông tin. 2. Đối tượng kiểm tra an ninh mạng bao gồm: a) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; b) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; c) Biện pháp bảo vệ bí mật nhà		Điều 21. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia 1. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia trong trường hợp sau đây: a) Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội; b) Khi có đề nghị của chủ quản hệ thống thông tin. 2. Đối tượng kiểm tra an ninh mạng bao gồm: a) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; b) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; c) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật. 3. Chủ quản hệ thống thông tin có	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật. 3. Chủ quản hệ thống thông tin có trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý. 4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức trong các trường hợp quy định tại khoản 1 Điều này. 5. Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ. Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin.		trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý. 4. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức trong các trường hợp quy định tại khoản 1 Điều này. 5. Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ. Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin. 6. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật. 7. Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng quy định tại Điều này.	

	6. Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật. 7. Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng quy định tại Điều này.			
22.	Điều 16. Phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế 1. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc. 2. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm: a) Kêu gọi, vận động, xúi giục,		Điều 22. Phòng ngừa, xử lý thông tin trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội 1. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc. 2. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm: a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018 VÀ BỔ SUNG THÊM MỘT SỐ NỘI DUNG MỚI

	đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự. 3. Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm: a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác. 4. Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm: a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán.		mất ổn định về an ninh, trật tự. 3. Thông tin trên không gian mạng có nội dung xâm phạm an ninh lãnh thổ, lợi ích của Nhà nước, phá hoại chính sách kinh tế - xã hội, cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: a) Phản ánh sai lệch, không chính xác về đường biên giới quốc gia chủ quyền lãnh thổ quốc gia Việt Nam; đăng tải, truyền đưa hình ảnh sai lệch, không chính xác, không đầy đủ về bản đồ Việt Nam hoặc thể hiện sai chủ quyền quốc gia Việt Nam; b) Tuyên truyền gây tổn hại trực tiếp hoặc gián tiếp đến quyền, lợi ích hợp pháp của Nhà nước về chính trị, kinh tế, xã hội, uy tín quốc tế; c) Kêu gọi, kích động phá hoại việc thực hiện các chính sách kinh tế - xã hội, gây cản trở việc thực thi của các chính sách; d) Kêu gọi, kích động phá hoại cơ sở vật chất - kỹ thuật của nước Cộng hòa xã hội chủ nghĩa Việt Nam. 4. Thông tin trên không gian mạng có nội dung phá hoại chính sách đoàn kết bao gồm: a) Gây mâu thuẫn, chia rẽ giữa các tầng lớp nhân dân, giữa nhân dân với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội; b) Kích động, gây hận thù, kỳ thị, chia	

	5. Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác. 6. Chủ quản hệ thống thông tin có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng. 7. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng biện pháp quy định tại các điểm h, i và l khoản 1 Điều 5 của Luật này để xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này. 8. Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin có trách		rẽ, ly khai dân tộc, xâm phạm quyền bình đẳng trong cộng đồng các dân tộc Việt Nam; c) Kích động, gây mâu thuẫn, chia rẽ người theo tôn giáo với người không theo tôn giáo, giữa người theo các tôn giáo khác nhau, chia rẽ các tín đồ tôn giáo với chính quyền nhân dân, với lực lượng vũ trang nhân dân hoặc các tổ chức chính trị - xã hội; d) Phá hoại, cản trở việc thực hiện chính sách đoàn kết quốc tế. 5. Thông tin trên không gian mạng có nội dung xâm phạm quyền, lợi ích hợp pháp của cá nhân bao gồm: a) Xúc phạm danh dự, uy tín, nhân phẩm của người khác; b) Xuyên tạc sai sự thật, gây ảnh hưởng đến danh dự, uy tín, nhân phẩm của người khác; c) Bịa đặt hoặc lan truyền những điều biết rõ là sai sự thật gây thiệt hại đến quyền, lợi ích hợp pháp của người khác; d) Bịa đặt người khác phạm tội và tố cáo họ trước cơ quan có thẩm quyền; c) Mạo danh, giả mạo thông tin, hình ảnh, giọng nói của cá nhân, gây ảnh hưởng đến uy tín, danh dự, nhân phẩm của cá nhân. 6. Thông tin trên không gian mạng có nội dung xâm phạm quyền, lợi ích hợp pháp của tổ chức bao gồm: a) Loan truyền thông tin xuyên tạc, bịa	

	nhiệm phối hợp với cơ quan chức năng xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này. 9. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều này phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật.		đặt, sai sự thật, gây ảnh hưởng đến uy tín, hoạt động bình thường của tổ chức; b) Kêu gọi, vận động, xúi giục tẩy chay sản phẩm, dịch vụ, hàng hóa, nhãn hàng, thương hiệu của tổ chức, doanh nghiệp, gây thiệt hại về vật chất, uy tín của doanh nghiệp, tổ chức; c) Mạo danh, giả mạo thông tin, hình ảnh, làm nhái sản phẩm, nhãn hiệu hàng hóa, thương hiệu của tổ chức, doanh nghiệp bằng cách sử dụng các tiện ích công nghệ, gây ảnh hưởng đến uy tín của tổ chức, doanh nghiệp. 7. Chủ quản hệ thống thông tin, doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung quy định tại các khoản khoản 1, 2, 3, 4, 5 và 6 Điều này trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng. 8. Lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng biện pháp quy định tại khoản 1 Điều 6 của Luật này để xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4, 5 và 6 Điều này.	

			9. Doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin có trách nhiệm phối hợp với cơ quan chức năng xử lý thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4, 5 và 6 Điều này. 10. Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4, 5 và 6 Điều này phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật.	
23.	Điều 17. Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng 1. Hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm: a) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá		Điều 23. Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng 1. Hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm: a) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng; c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; d) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật; đ) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại; e) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.		và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng; c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; d) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật; đ) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại; e) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư. 2. Chủ quản hệ thống thông tin có trách nhiệm sau đây: a) Kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng;	

	2. Chủ quản hệ thống thông tin có trách nhiệm sau đây: a) Kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng; b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này; c) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin. 3. Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị		b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này; c) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin. 3. Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước. 4. Bộ Công an có trách nhiệm sau đây, trừ quy định tại khoản 5 và khoản 6 Điều này: a) Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp; b) Kiểm tra an ninh mạng đối với thiết	

	khác hoặc trao đổi trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước. 4. Bộ Công an có trách nhiệm sau đây, trừ quy định tại khoản 5 và khoản 6 Điều này: a) Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp; b) Kiểm tra an ninh mạng đối với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia; c) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước; d) Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng; đ) Tham gia nghiên cứu, sản		bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng quốc gia; c) Giám sát an ninh mạng đối với hệ thống thông tin quan trọng quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước; d) Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng; đ) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước theo quy định của pháp luật bảo vệ bí mật nhà nước và pháp luật cơ yếu; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao; e) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng quốc gia; g) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng quy định tại khoản 2 Điều 45 của Luật này. 5. Bộ Quốc phòng có trách nhiệm thực	

	xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao; e) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; g) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng quy định tại khoản 2 Điều 30 của Luật này. 5. Bộ Quốc phòng có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin quân sự. 6. Ban Cơ yếu Chính phủ có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.		hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin quân sự. 6. Ban Cơ yếu Chính phủ có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều này đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ; có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.	
24.	Điều 18. Phòng, chống hành vi		Điều 24. Phòng, chống hành vi sử	- KẾ THỪA LUẬT AN

	sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội 1. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội bao gồm: a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 và hành vi quy định tại khoản 1 Điều 17 của Luật này; b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng; c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; d) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy		dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội 1. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, bao gồm: a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 Điều 20; b) Thực hiện hành vi quy định tại khoản 1 Điều 23 của Luật này. 2. Hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để xâm phạm trật tự, an an toàn xã hội bao gồm: a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2 Điều 21 của Luật này; b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng; c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; làm giả con dấu, tài liệu hoặc giấy tờ khác của cơ	NINH MẠNG NĂM 2018 VÀ BỔ SUNG THÊM MỘT SỐ NỘI DUNG MỚI

	định của pháp luật; đ) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật; e) Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội. 2. Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.		quan, tổ chức d) Tuyên truyền, quảng cáo, mua bán trái phép vũ khí, vật liệu nổ, công cụ hỗ trợ, pháo nổ; ma túy, tiền chất ma túy, chất gây nghiện, chất hướng thần; động vật hoang dã, nguy cấp, quý, hiếm và các hàng hóa, dịch vụ khác thuộc danh mục cấm theo quy định của pháp luật; môi giới mại dâm; truyền bá văn hóa phẩm đồi trụy; lạm dụng tình dục trẻ em; quấy rối tình dục; đ) Thiết lập, cung cấp dịch vụ hoặc hỗ trợ vận hành, kinh doanh, giao dịch, mua bán, tiếp thị trực tuyến cho sàn giao dịch, website, ứng dụng trái phép trên không gian mạng, bao gồm: sàn thương mại điện tử, website, ứng dụng bán hàng, cung cấp dịch vụ thương mại điện tử; sàn giao dịch dựa trên chỉ số các loại hàng hóa; sàn giao dịch tài sản số, kinh doanh theo phương thức đa cấp; e) Sử dụng danh tính giả, thông tin của người khác, giấy tờ, hồ sơ giả để thành lập doanh nghiệp, thiết lập, đăng ký tài khoản ngân hàng, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và tài khoản số khác; thu thập, tàng trữ, trao đổi, mua bán, tặng cho, công khai hóa trái phép dữ liệu, thông tin tài khoản ngân hàng, thẻ ngân hàng, tài khoản ví điện tử, tài khoản chứng khoán, tài khoản bảo hiểm, tài khoản thuế và các loại tài khoản số khác;	

			g) Quảng cáo, buôn bán hàng giả, hàng hóa nhập lậu, không rõ nguồn gốc, xuất xứ; hàng hóa lưu thông trong nước bị áp dụng biện pháp khẩn cấp; hàng hóa quá hạn sử dụng; i) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật; l) Hành vi khác sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao vi phạm pháp luật về trật tự, an toàn xã hội. 3. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an, Bộ Quốc phòng và cơ quan chức năng liên quan có trách nhiệm thực hiện các biện pháp quy định tại khoản 1 Điều 6 của Luật này để đấu tranh, phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao để vi phạm pháp luật về trật tự, an toàn xã hội. 4. Chính phủ quy định chi tiết về phòng, chống tội phạm sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử, công nghệ cao xâm phạm trật tự, an toàn xã hội.	
25.	Điều 29. Bảo vệ trẻ em trên không gian mạng 1. Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng.		Điều 25. Phòng, chống xâm hại trẻ em trên không gian mạng 1. Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia, tương tác trên không gian mạng.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	2. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý. 3. Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin có nội dung gây nguy hại cho trẻ em theo quy định của Luật này và pháp luật về trẻ em. 4. Cơ quan, tổ chức, cha mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, bảo vệ trẻ em khi tham		2. Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm: kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em hoặc xâm phạm đến trẻ em hoặc xâm phạm quyền trẻ em, quyền của người yếu thế; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em hoặc xâm phạm đến trẻ em hoặc xâm phạm đến quyền trẻ em; xây dựng, triển khai các hệ thống kỹ thuật hỗ trợ hoạt động ngăn chặn nội dung xâm hại trẻ em trên không gian mạng; điều phối các cơ quan, tổ chức, doanh nghiệp thực hiện ngăn chặn các nguồn phát tán thông tin xâm hại trẻ em trên không gian mạng; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý. 3. Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin mạng gây nguy hại cho trẻ em theo quy định của Luật này và pháp luật về trẻ em. 4. Cơ quan, tổ chức, cha mẹ, con cái, người giám hộ, giáo viên, người chăm	

	gia không gian mạng theo quy định của pháp luật về trẻ em. 5. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.		sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, người yếu thế, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em. 5. Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.	
26.		Điều 11. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại 1. Cơ quan, tổ chức, cá nhân có trách nhiệm thực hiện phòng ngừa, ngăn chặn phần mềm độc hại theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền. 2. Chủ quản hệ thống thông tin quan trọng quốc gia triển khai hệ thống kỹ thuật nghiệp vụ nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời phần mềm độc hại. 3. Doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình và báo cáo cơ quan nhà nước có thẩm quyền theo quy định của pháp luật. 4. Doanh nghiệp cung cấp dịch vụ	Điều 26. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại 1. Cơ quan, tổ chức, cá nhân có trách nhiệm chủ động phòng ngừa, ngăn chặn phần mềm độc hại và thực hiện phòng ngừa, ngăn chặn theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền. 2. Chủ quản hệ thống thông tin quan trọng quốc gia triển khai hệ thống kỹ thuật nhằm phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời phần mềm độc hại. 3. Tổ chức, doanh nghiệp cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin phải có hệ thống lọc phần mềm độc hại trong quá trình gửi, nhận, lưu trữ thông tin trên hệ thống của mình và báo cáo cơ quan nhà nước có thẩm quyền theo quy định của pháp luật. 4. Doanh nghiệp cung cấp dịch vụ	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		Internet có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền. 5. Bộ Thông tin và Truyền thông chủ trì, phối hợp với Bộ Quốc phòng, Bộ Công an và bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh quốc gia.	Internet có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại và xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền. 5. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và bộ, ngành có liên quan tổ chức phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại gây ảnh hưởng đến quốc phòng, an ninh quốc gia.	
27.	Điều 19. Phòng, chống tấn công mạng 1. Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm: a) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; c) Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn		Điều 27. Phòng, chống tấn công mạng 1. Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng bao gồm: a) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của không gian mạng; c) Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; d) Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; d) Xâm nhập, tạo ra hoặc khai thác điểm yếu, lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính; đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật; e) Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử. 2. Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi quy định tại các điểm a, b, c, d và e khoản 1 Điều này đối với hệ thống thông tin thuộc phạm vi quản lý. 3. Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm		hệ thống để chiếm đoạt thông tin, thu lợi bất chính; đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng gây hại mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật; e) Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử. 2. Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi quy định tại các điểm a, b, c, d và e khoản 1 Điều này đối với hệ thống thông tin thuộc phạm vi quản lý. 3. Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia	

	phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan. 4. Trách nhiệm phòng, chống tấn công mạng được quy định như sau: a) Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội trên phạm vi cả nước, trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan		tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan. 4. Trách nhiệm phòng, chống tấn công mạng được quy định như sau: a) Bộ Công an chủ trì, phối hợp với bộ, ngành, địa phương có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội trên phạm vi cả nước, trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.	

	thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều này đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.			
28.	Điều 20. Phòng, chống khủng bố mạng 1. Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật này, Điều 29 của Luật An toàn thông tin mạng và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng. 2. Chủ quản hệ thống thông tin thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng. 3. Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực		Điều 28. Phòng, chống khủng bố mạng 1. Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật này và pháp luật về phòng, chống khủng bố để xử lý khủng bố mạng. 2. Chủ quản hệ thống thông tin thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng. 3. Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng. 4. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	lượng chuyên trách bảo vệ an ninh mạng. 4. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp vô hiệu hóa nguồn khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra đối với hệ thống thông tin, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này. 5. Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự. 6. Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.		dụng biện pháp vô hiệu hóa nguồn khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra đối với hệ thống thông tin, trừ trường hợp quy định tại khoản 5 và khoản 6 Điều này. 5. Bộ Quốc phòng chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự. 6. Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ.	
29.	Điều 21. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng 1. Tình huống nguy hiểm về an ninh mạng bao gồm: a) Xuất hiện thông tin kích		Điều 29. Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng 1. Tình huống nguy hiểm về an ninh mạng bao gồm: a) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố; b) Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; c) Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao; d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia; đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 2. Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng; b) Doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ		bạo loạn, phá rối an ninh, khủng bố; b) Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; c) Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao; d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia; đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. 2. Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng được quy định như sau: a) Lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng; b) Doanh nghiệp viễn thông, Internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện,	

	trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng. 3. Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm: a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan; c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng; d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế; e) Bố trí lực lượng, phương tiện		xử lý tình huống nguy hiểm về an ninh mạng. 3. Biện pháp xử lý tình huống nguy hiểm về an ninh mạng bao gồm: a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan; c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng; d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế; e) Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng; g) Biện pháp khác theo quy định của Luật An ninh quốc gia. 4. Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau: a) Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và áp dụng ngay các biện pháp quy định tại điểm a và điểm b khoản 3 Điều này;	

	ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng; g) Biện pháp khác theo quy định của Luật An ninh quốc gia. 4. Việc xử lý tình huống nguy hiểm về an ninh mạng được quy định như sau: a) Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và áp dụng ngay các biện pháp quy định tại điểm a và điểm b khoản 3 Điều này; b) Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể. Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; c) Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá		b) Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể. Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; c) Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp quy định tại khoản 3 Điều này để xử lý tình huống nguy hiểm về an ninh mạng; d) Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.	

	nhân có liên quan áp dụng các biện pháp quy định tại khoản 3 Điều này để xử lý tình huống nguy hiểm về an ninh mạng; d) Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.			
30.	Điều 22. Đấu tranh bảo vệ an ninh mạng 1. Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội. 2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm: a) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia; b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia; c) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an		Điều 30. Đấu tranh bảo vệ an ninh mạng 1. Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội. 2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm: a) Giám sát thông tin mạng và phòng ngừa, đấu tranh, xử lý tổ chức, cá nhân có hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội; b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng quốc gia; c) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	toàn xã hội; d) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội. 3. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.		d) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội. 3. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.	
31.		Điều 28. Trách nhiệm của tổ chức, cá nhân trong việc ngăn chặn xung đột thông tin trên mạng 1. Tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm sau đây: a) Ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài; b) Ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng; c) Loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài. 2. Chính phủ quy định chi tiết về	Điều 31. Ngăn chặn xung đột thông tin trên mạng 1. Ngăn chặn xung đột thông tin trên mạng là việc thực hiện các biện pháp công nghệ, kỹ thuật để giám sát, phát hiện, cảnh báo, xác định nguồn gốc, chặn lọc, khắc phục và loại trừ xung đột thông tin trên mạng. 2. Nội dung ngăn chặn xung đột thông tin trên mạng bao gồm: a) Giám sát, phát hiện, cảnh báo, xung đột thông tin trên mạng; b) Xác định nguồn gốc xung đột thông tin trên mạng; c) Chặn lọc, khắc phục và loại trừ xung đột thông tin trên mạng; d) Thông tin, tuyên truyền, giáo dục và hợp tác quốc tế về ngăn chặn xung đột thông tin trên mạng. 3. Tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm sau đây: a) Ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình;	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018), BỔ SUNG THÊM NỘI DUNG CÓ LIÊN QUAN TẠI LUẬT AN NINH MẠNG

		ngăn chặn xung đột thông tin trên mạng.	hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài; b) Ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng; c) Loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài. 4. Chính phủ quy định chi tiết về ngăn chặn xung đột thông tin trên mạng.	
32.		Điều 9. Phân loại thông tin 1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp. 2. Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước. Cơ quan, tổ chức sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải có trách nhiệm xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.	Điều 32. Phân loại thông tin 1. Cơ quan, tổ chức sở hữu thông tin phân loại thông tin theo mức độ nhạy cảm của thông tin, theo tính chất và lĩnh vực của thông tin, theo tình trạng và sự thay đổi của thông tin, theo mức độ quyền truy cập để có biện pháp bảo vệ phù hợp. 2. Thông tin thuộc phạm vi bí mật nhà nước được phân loại và bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước. Cơ quan, tổ chức sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải có trách nhiệm xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

			và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.	
33.		Điều 10. Quản lý gửi thông tin 1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây: a) Không giả mạo nguồn gốc gửi thông tin; b) Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan. 2. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật. 3. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ ứng dụng viễn thông và doanh nghiệp cung cấp dịch vụ công nghệ thông tin gửi thông tin có trách nhiệm sau đây: a) Tuân thủ quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của tổ chức, cá nhân; b) Áp dụng biện pháp ngăn chặn, xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật; c) Có phương thức để người tiếp nhận thông tin có khả năng từ chối việc tiếp nhận thông tin;	Điều 33. Quản lý gửi thông tin trên mạng 1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây: a) Không giả mạo nguồn gốc gửi thông tin; b) Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan. 2. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật. 3. Nhà cung cấp dịch vụ có trách nhiệm sau đây: a) Tuân thủ quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của tổ chức, cá nhân. b) Áp dụng biện pháp ngăn chặn, xử lý khi nhận được thông báo của tổ chức, cá nhân về việc gửi thông tin vi phạm quy định của pháp luật. c) Có phương thức để người tiếp nhận thông tin có khả năng từ chối việc tiếp nhận thông tin. d) Cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết để cơ quan nhà	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		d) Cung cấp điều kiện kỹ thuật và nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ quản lý, bảo đảm an toàn thông tin mạng khi có yêu cầu.	nước có thẩm quyền thực hiện nhiệm vụ quản lý, bảo đảm an ninh mạng khi có yêu cầu. đ) Áp dụng cơ chế kiểm soát tự động để kiểm soát việc gửi thông tin trên mạng. e) Tăng cường bảo mật thông tin liên quan đến giao dịch trực tuyến để bảo đảm an toàn cho các giao dịch thông qua các phương thức xác thực đa yếu tố, mã hóa thông tin và bảo vệ thông tin tài chính của người dùng khi gửi, nhận thông tin giao dịch trực tuyến. g) Cung cấp thông tin đầy đủ về quyền và nghĩa vụ của người tiếp nhận thông tin khi họ từ chối thông tin, cũng như các hậu quả và quyền lợi liên quan đến việc tiếp nhận hoặc từ chối nhận thông tin.	
34.	Điều 23. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương 1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm: a) Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng;		Điều 34. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương 1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm: a) Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng Internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng; b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý; c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng; d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ; đ) Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin; e) Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng. 2. Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai		mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý; c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng; d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ; đ) Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin; e) Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng. 2. Người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.	

	hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.			
35.	Điều 25. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế 1. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia. 2. Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế có trách nhiệm sau đây: a) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền; b) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có		Điều 35. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế 1. Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia. 2. Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế có trách nhiệm sau đây: a) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền; b) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	đề nghị.			
36.	Điều 26. Bảo đảm an ninh thông tin trên không gian mạng 1. Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật này và thông tin khác có nội dung xâm phạm an ninh quốc gia. 2. Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm sau đây: a) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật này trên		Điều 36. Bảo đảm an ninh thông tin trên không gian mạng 1. Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin có nội dung được quy định tại khoản 1, 2, 3, 4 Điều 20 và khoản 1, 2 Điều 21 Luật này và thông tin khác có nội dung xâm phạm an ninh quốc gia. 2. Doanh nghiệp trong nước và nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm sau đây: a) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chậm nhất là 24 giờ khi có yêu cầu bằng văn bản hoặc thư điện tử, điện thoại hoặc một loại hình thức trao đổi khác đã được xác nhận để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, đe dọa tính mạng con người, yêu cầu cung cấp thông tin chậm nhất là 03 giờ. b) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin gỡ bỏ dịch vụ, ứng	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	dịch vụ hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ; c) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông. 3. Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về		dụng có nội dung vi phạm quy định của Luật này trên dịch vụ, kho ứng dụng hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của pháp luật (của Chính phủ); trường hợp khẩn cấp đe dọa xâm hại an ninh quốc gia, yêu cầu ngăn chặn, xóa bỏ thông tin chậm nhất là 06 giờ. c) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng đối với thông tin có nội dung quy định tại khoản 1, 2, 3, 4 Điều 20 và khoản 1, 2 Điều 21 Luật này khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an. d) Lưu trữ thông tin cá nhân của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tạo ra, bao gồm: tên tài khoản, thời gian sử dụng dịch vụ, thông tin thanh toán phí sử dụng dịch vụ, địa chỉ IP truy cập và các dữ liệu liên quan khác trong suốt quá trình sử dụng đến 02 năm sau khi người dùng kết thúc việc sử dụng dịch vụ. 3. Doanh nghiệp trong nước và ngoài	

	mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. 4. Chính phủ quy định chi tiết khoản 3 Điều này.		nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải áp dụng các biện pháp bảo vệ dữ liệu theo quy định của pháp luật và lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. 4. Chính phủ quy định chi tiết Khoản 2, Khoản 3 Điều này.	
37.			Điều 37. Bảo đảm an ninh dữ liệu 1. An ninh dữ liệu là sự bảo đảm an toàn, bí mật, khả dụng của dữ liệu chuyên ngành của cơ quan, tổ chức nhà nước; phòng, chống việc sử dụng, khai thác trái phép, chiếm đoạt, cố ý làm sai lệch, tiêu hủy dữ liệu chuyên ngành, phá hoại cơ sở dữ liệu chuyên ngành của cơ quan, tổ chức nhà nước, gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội. 2. Cơ quan, tổ chức, doanh nghiệp nhà nước thiết lập cơ sở, trung tâm, hệ thống lưu trữ dữ liệu chuyên ngành có trách nhiệm xây dựng và thực hiện hệ thống quản lý an ninh dữ liệu sau đây:	BỔ SUNG MỚI

			a) Thiết lập quy trình, quy định nội bộ về bảo vệ an ninh dữ liệu; b) Áp dụng biện pháp, tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, mật mã, mã hóa, phân quyền truy cập, kiểm tra giám sát truy cập, sao lưu và khôi phục dữ liệu. c) Có cơ chế kiểm soát chặt chẽ nhân sự trực tiếp tham gia xử lý dữ liệu chuyên ngành. c) Kiểm tra, đánh giá rủi ro định kỳ đối với hệ thống, cơ sở, trung tâm lưu trữ dữ liệu chuyên ngành nhằm phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ đe dọa an ninh dữ liệu. 3. Trách nhiệm kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu lưu trong hệ thống thông tin quan trọng quốc gia, các cơ sở, trung tâm dữ liệu chuyên ngành của cơ quan, tổ chức, doanh nghiệp nhà nước trừ trường hợp quy định tại điểm b và điểm c khoản này; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra, đánh giá điều kiện đảm bảo an ninh dữ liệu lưu trong hệ thống thông tin quân sự, cơ sở, trung tâm dữ liệu thuộc Bộ Quốc phòng quản lý. 4. Chính phủ quy định chi tiết khoản 1,	

			khoản 2, khoản 3 Điều này.	
38.		**Điều 37. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng** 1. Tiêu chuẩn an toàn thông tin mạng gồm tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn nước ngoài, tiêu chuẩn quốc gia và tiêu chuẩn cơ sở đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng được công bố, thừa nhận áp dụng tại Việt Nam. 2. Quy chuẩn kỹ thuật an toàn thông tin mạng gồm quy chuẩn kỹ thuật quốc gia và quy chuẩn kỹ thuật địa phương đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng được xây dựng, ban hành và áp dụng tại Việt Nam.	Điều 38. Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng 1. Tiêu chuẩn an ninh mạng gồm tiêu chuẩn quốc tế, tiêu chuẩn khu vực, tiêu chuẩn nước ngoài, tiêu chuẩn quốc gia và tiêu chuẩn cơ sở về an ninh mạng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng được công bố, thừa nhận áp dụng tại Việt Nam. 2. Quy chuẩn kỹ thuật an ninh mạng gồm quy chuẩn kỹ thuật quốc gia và quy chuẩn kỹ thuật địa phương về an ninh mạng đối với hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng được xây dựng, ban hành và áp dụng tại Việt Nam.	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),
39.		**Điều 38. Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng** 1. Chứng nhận hợp quy về an toàn thông tin mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng phù hợp với quy chuẩn kỹ thuật an toàn thông tin mạng.	Điều 39. Quản lý tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng 1. Chứng nhận hợp quy về an ninh mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng phù hợp với quy chuẩn kỹ thuật an ninh mạng.	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		2. Công bố hợp quy về an toàn thông tin mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng với quy chuẩn kỹ thuật an toàn thông tin mạng. 3. Chứng nhận hợp chuẩn về an toàn thông tin mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng phù hợp với tiêu chuẩn an toàn thông tin mạng. 4. Công bố hợp chuẩn về an toàn thông tin mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an toàn thông tin mạng với tiêu chuẩn an toàn thông tin mạng. 5. 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 toàn thông tin mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật. 6. Bộ Thông tin và Truyền thông có trách nhiệm sau đây: a) Xây dựng dự thảo tiêu chuẩn quốc gia an toàn thông tin mạng, trừ tiêu chuẩn quốc gia quy định tại	2. Công bố hợp quy về an ninh mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng với quy chuẩn kỹ thuật an ninh mạng. 3. Chứng nhận hợp chuẩn về an ninh mạng là việc tổ chức chứng nhận sự phù hợp chứng nhận hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng phù hợp với tiêu chuẩn an ninh mạng. 4. Công bố hợp chuẩn về an ninh mạng là việc tổ chức, doanh nghiệp công bố về sự phù hợp của hệ thống thông tin, phần cứng, phần mềm, hệ thống quản lý, vận hành an ninh mạng, sản phẩm, dịch vụ công nghệ thông tin và thiết bị kết nối mạng an ninh mạng với tiêu chuẩn an ninh mạng. 5. 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; thẩm định quy chuẩn kỹ thuật quốc gia về an ninh mạng theo quy định của pháp luật về tiêu chuẩn, quy chuẩn kỹ thuật. 6. Bộ Công an có trách nhiệm sau đây: a) Xây dựng dự thảo tiêu chuẩn quốc gia về an ninh mạng, trừ tiêu chuẩn	

		khoản 7 Điều này; b) Ban hành quy chuẩn kỹ thuật quốc gia an toàn thông tin mạng, trừ quy chuẩn quốc gia quy định tại khoản 7 Điều này; quy định về đánh giá hợp quy về an toàn thông tin mạng; c) Quản lý chất lượng sản phẩm, dịch vụ an toàn thông tin mạng, trừ sản phẩm, dịch vụ mật mã dân sự; d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an toàn thông tin mạng, trừ tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự. 7. Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự trình cơ quan nhà nước có thẩm quyền công bố và hướng dẫn thực hiện; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự. 8. Ủy ban nhân dân cấp tỉnh xây dựng, ban hành và hướng dẫn thực hiện quy chuẩn kỹ thuật địa phương	quốc gia quy định tại khoản 7 Điều này; b) Xây dựng và ban hành quy chuẩn kỹ thuật quốc gia về an ninh mạng, trừ quy chuẩn quốc gia quy định tại khoản 7 Điều này; c) Quản lý chất lượng sản phẩm, dịch vụ an ninh mạng; d) Đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng, trừ tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự. 7. Ban Cơ yếu Chính phủ có trách nhiệm giúp Bộ trưởng Bộ Quốc phòng chủ trì, phối hợp Bộ Công an xây dựng dự thảo tiêu chuẩn quốc gia đối với sản phẩm, dịch vụ mật mã dân sự; xây dựng, trình Bộ trưởng Bộ Quốc phòng ban hành quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp đối với sản phẩm, dịch vụ mật mã dân sự. 8. Ủy ban nhân dân cấp tỉnh 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 an ninh mạng trên địa bàn.	

		về an toàn thông tin mạng; quản lý chất lượng sản phẩm, dịch vụ an toàn thông tin mạng trên địa bàn.		
40.		**Điều 39. Đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng** 1. Việc đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng được thực hiện trong các trường hợp sau đây: a) Trước khi tổ chức, cá nhân đưa sản phẩm an toàn thông tin mạng vào lưu thông trên thị trường phải thực hiện chứng nhận hợp quy hoặc công bố hợp quy và sử dụng dấu hợp quy; b) Phục vụ hoạt động quản lý nhà nước về an toàn thông tin mạng. 2. Việc đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng phục vụ hệ thống thông tin quan trọng quốc gia và phục vụ hoạt động quản lý nhà nước về an toàn thông tin mạng được thực hiện tại tổ chức chứng nhận sự phù hợp do Bộ trưởng Bộ Thông tin và Truyền thông chỉ định. 3. Việc đánh giá hợp chuẩn, hợp quy đối với sản phẩm, dịch vụ mật mã dân sự được thực hiện tại tổ chức chứng nhận sự phù hợp do Bộ trưởng Bộ Quốc phòng chỉ định. 4. Việc thừa nhận kết quả đánh giá hợp chuẩn, hợp quy về an toàn thông tin mạng giữa Việt Nam với quốc gia, vùng lãnh thổ khác, giữa tổ chức chứng nhận sự phù hợp của	Điều 40. 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 phải thực hiện chứng nhận hợp quy hoặc công bố hợp quy và sử dụng dấu hợp quy; b) Phục vụ hoạt động quản lý nhà nước về an ninh mạng. 2. Việc đánh giá hợp chuẩn, hợp quy về an ninh mạng phục vụ hệ thống thông tin quan trọng quốc gia và phục vụ hoạt động quản lý nhà nước về an ninh mạng được thực hiện tại tổ chức chứng nhận hợp chuẩn, hợp quy do Bộ trưởng Bộ Công an chỉ định. 3. 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.	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		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.		
41.		**Điều 41. Sản phẩm, dịch vụ trong lĩnh vực an toàn thông tin mạng** 1. Dịch vụ an toàn thông tin mạng gồm: a) Dịch vụ kiểm tra, đánh giá an toàn thông tin mạng; b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự; c) Dịch vụ mật mã dân sự; d) Dịch vụ chứng thực chữ ký điện tử; đ) Dịch vụ tư vấn an toàn thông tin mạng; e) Dịch vụ giám sát an toàn thông tin mạng; g) Dịch vụ ứng cứu sự cố an toàn thông tin mạng; h) Dịch vụ khôi phục dữ liệu; i) Dịch vụ phòng ngừa, chống tấn công mạng; k) Dịch vụ an toàn thông tin mạng khác. 2. Sản phẩm an toàn thông tin mạng gồm: a) Sản phẩm mật mã dân sự; b) Sản phẩm kiểm tra, đánh giá an toàn thông tin mạng; c) Sản phẩm giám sát an toàn thông	Điều 41. Sản phẩm, dịch vụ an ninh mạng 1. Dịch vụ an ninh mạng gồm: a) Dịch vụ kiểm tra, đánh giá an ninh mạng; b) Dịch vụ bảo mật thông tin không sử dụng mật mã dân sự; c) Dịch vụ mật mã dân sự; d) Dịch vụ chứng thực chữ ký điện tử; đ) Dịch vụ tư vấn an ninh mạng; e) Dịch vụ giám sát an ninh mạng; g) Dịch vụ ứng cứu sự cố an ninh mạng; h) Dịch vụ khôi phục dữ liệu; i) Dịch vụ phòng ngừa, chống tấn công mạng; k) Dịch vụ ẩn danh trên không gian mạng; l) Dịch vụ săn tìm lỗ hổng có thưởng; m) Dịch vụ an ninh mạng khác. 2. Sản phẩm an ninh mạng gồm: a) Sản phẩm mật mã dân sự; b) Sản phẩm kiểm tra, đánh giá an ninh mạng; c) Sản phẩm giám sát an ninh mạng; d) Sản phẩm chống tấn công, xâm nhập; e) Sản phẩm an ninh mạng khác.	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		tin mạng; d) Sản phẩm chống tấn công, xâm nhập; đ) Sản phẩm an toàn thông tin mạng khác. 3. Chính phủ quy định chi tiết danh mục sản phẩm, dịch vụ an toàn thông tin mạng quy định tại điểm k khoản 1 và điểm đ khoản 2 Điều này.	3. Chính phủ quy định chi tiết danh mục sản phẩm, dịch vụ mật mã dân sự và các danh mục sản phẩm, dịch vụ an ninh mạng khác quy định tại khoản 1, 2 Điều này.	
42.		**Điều 42. Điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng** 1. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trừ sản phẩm, dịch vụ quy định tại các điểm a, b, c, d khoản 1 và điểm a khoản 2 Điều 41 của Luật này, khi đáp ứng đủ các điều kiện sau đây: a) Phù hợp với chiến lược, quy hoạch, kế hoạch phát triển an toàn thông tin mạng quốc gia; b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ an toàn thông tin mạng; c) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng được yêu cầu chuyên môn về an toàn thông tin; d) Có phương án kinh doanh phù hợp. 2. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ kiểm tra,	Điều 42. Điều kiện cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng 1. Doanh nghiệp được cấp Giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng, trừ sản phẩm, dịch vụ quy định tại các điểm a, b, c, d khoản 1 và điểm a khoản 2 Điều 37 của Luật này, khi đáp ứng đủ các điều kiện sau đây: a) Phù hợp với chiến lược, quy hoạch, kế hoạch phát triển an ninh mạng quốc gia; b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ an ninh mạng; c, Có nhân sự chịu trách nhiệm về bảo đảm an ninh mạng đáp ứng yêu cầu về kiến thức, kỹ năng về bảo đảm an ninh mạng, được cơ quan có thẩm quyền chứng nhận theo quy định; d) Có phương án kinh doanh phù hợp; đ) Có đăng ký ngành, nghề kinh doanh phù hợp; e) Có đội ngũ quản lý, điều hành, kỹ	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		đánh giá an toàn thông tin mạng khi đáp ứng đủ các điều kiện sau đây: a) Các điều kiện quy định tại khoản 1 Điều này; b) Là doanh nghiệp được thành lập và hoạt động hợp pháp trên lãnh thổ Việt Nam, trừ doanh nghiệp có vốn đầu tư nước ngoài; c) Người đại diện theo pháp luật, đội ngũ quản lý, điều hành, kỹ thuật là công dân Việt Nam thường trú tại Việt Nam; d) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật; đ) Có phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ; e) Đội ngũ quản lý, điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về kiểm tra, đánh giá an toàn thông tin. 3. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ bảo mật thông tin không sử dụng mật mã dân sự khi đáp ứng đủ các điều kiện sau đây: a) Các điều kiện quy định tại các điểm a, b, c, d và đ khoản 2 Điều này; b) Đội ngũ quản lý điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về bảo mật thông tin. 4. Chính phủ quy định chi tiết Điều này.	thuật đáp ứng được yêu cầu chuyên môn về an ninh mạng, nhân thân, lý lịch rõ ràng. 2. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ kiểm tra, đánh giá, giám sát an ninh mạng khi đáp ứng đủ các điều kiện sau đây: a) Các điều kiện quy định tại khoản 1 Điều này; b) Là doanh nghiệp được thành lập và hoạt động hợp pháp trên lãnh thổ Việt Nam, trừ doanh nghiệp có vốn đầu tư nước ngoài; c) Người đại diện theo pháp luật, đội ngũ quản lý, điều hành, kỹ thuật là công dân Việt Nam thường trú tại Việt Nam; d) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật; đ) Có phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ; e) Đội ngũ quản lý, điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên môn về kiểm tra, đánh giá an ninh mạng. 3. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ bảo mật thông tin không sử dụng mật mã dân sự khi đáp ứng đủ các điều kiện sau đây: a) Các điều kiện quy định tại các điểm a, b, c, d và đ khoản 2 Điều này; b) Đội ngũ quản lý điều hành, kỹ thuật có văn bằng hoặc chứng chỉ chuyên	

			môn về bảo mật thông tin. 4. Doanh nghiệp được cấp Giấy phép kinh doanh dịch vụ mật mã dân sự khi đáp ứng đủ các yêu cầu sau đây: a) Có đội ngũ quản lý, điều hành, kỹ thuật đáp ứng yêu cầu chuyên môn về bảo mật, an ninh mạng; b) Có hệ thống trang thiết bị, cơ sở vật chất phù hợp với quy mô cung cấp sản phẩm, dịch vụ mật mã dân sự; c) Có phương án kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật; d) Có phương án bảo mật và an ninh mạng trong quá trình quản lý và cung cấp sản phẩm, dịch vụ mật mã dân sự; đ) Có phương án kinh doanh phù hợp; e) Sản phẩm mật mã dân sự phải được kiểm định, chứng nhận hợp quy trước khi lưu thông trên thị trường. 5. Chính phủ quy định chi tiết về việc kinh doanh sản phẩm, dịch vụ an ninh mạng và mật mã dân sự.	
43.		**Điều 46. Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng** 1. Quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm. 2. Lập, lưu giữ và bảo mật thông tin của khách hàng. 3. Định kỳ hằng năm báo cáo Bộ Thông tin và Truyền thông về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an toàn	Điều 43. Trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng 1. Quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, báo cáo Bộ Công an về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng khi có yêu cầu. 2. Lập, lưu giữ và bảo mật thông tin của khách hàng. 3. Định kỳ hằng năm báo cáo Bộ Công	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		thông tin mạng trước ngày 31 tháng 12. 4. Từ chối cung cấp sản phẩm, dịch vụ an toàn thông tin mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an toàn thông tin mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp. 5. Tạm ngừng hoặc ngừng cung cấp sản phẩm, dịch vụ an toàn thông tin mạng để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của cơ quan nhà nước có thẩm quyền. 6. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nghiệp vụ khi có yêu cầu.	an/Ủy ban nhân dân tỉnh, thành phố về tình hình kinh doanh, xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng trước ngày 31 tháng 12. 4. Từ chối cung cấp sản phẩm, dịch vụ an ninh mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an ninh mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp. 5. Tạm ngừng hoặc ngừng cung cấp sản phẩm, dịch vụ an ninh mạng để bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội theo yêu cầu của cơ quan nhà nước có thẩm quyền. 6. Phối hợp, tạo điều kiện cho cơ quan nhà nước có thẩm quyền thực hiện các biện pháp nghiệp vụ khi có yêu cầu.	
44.		**Điều 47. Nguyên tắc quản lý nhập khẩu sản phẩm an toàn thông tin mạng** 1. Việc quản lý nhập khẩu đối với sản phẩm an toàn thông tin mạng được thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan. 2. Việc nhập khẩu sản phẩm an toàn thông tin mạng của cơ quan, tổ chức, cá nhân được hưởng quyền ưu đãi, miễn trừ ngoại giao thực hiện theo quy định của pháp luật về hải quan, pháp luật về ưu đãi, miễn trừ dành	Điều 44. Nguyên tắc quản lý xuất khẩu, nhập khẩu sản phẩm, dịch vụ an ninh mạng 1. Việc quản lý xuất khẩu, nhập khẩu đối với sản phẩm an ninh mạng được thực hiện theo quy định của Luật này và quy định khác của pháp luật có liên quan. 2. Việc xuất khẩu, nhập khẩu sản phẩm an ninh mạng của cơ quan, tổ chức, cá nhân được hưởng quyền ưu đãi, miễn trừ ngoại giao thực hiện theo quy định của pháp luật về hải quan, pháp luật về ưu đãi, miễn trừ dành cho cơ quan đại	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		cho cơ quan đại diện ngoại giao, cơ quan lãnh sự của nước ngoài và cơ quan đại diện của tổ chức quốc tế liên Chính phủ tại Việt Nam. 3. Trong trường hợp Việt Nam chưa có quy chuẩn kỹ thuật an toàn thông tin mạng tương ứng đối với sản phẩm an toàn thông tin mạng nhập khẩu thì áp dụng theo thỏa thuận quốc tế, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.	diện ngoại giao, cơ quan lãnh sự của nước ngoài và cơ quan đại diện của tổ chức quốc tế liên Chính phủ tại Việt Nam. 3. Trong trường hợp Việt Nam chưa có quy chuẩn kỹ thuật an ninh mạng tương ứng đối với sản phẩm an ninh mạng nhập khẩu thì áp dụng theo thỏa thuận quốc tế, điều ước quốc tế mà Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên.	
45.	**Điều 27. Nghiên cứu, phát triển an ninh mạng** 1. Nội dung nghiên cứu, phát triển an ninh mạng bao gồm: a) Xây dựng hệ thống phần mềm, trang thiết bị bảo vệ an ninh mạng; b) Phương pháp thẩm định phần mềm, trang thiết bị bảo vệ an ninh mạng đạt chuẩn và hạn chế tồn tại điểm yếu, lỗ hổng bảo mật, phần mềm độc hại; c) Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng; d) Phương pháp bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; khả năng bảo mật khi truyền đưa thông tin trên không gian mạng;		Điều 45. Nghiên cứu, phát triển an ninh mạng 1. Nội dung nghiên cứu, phát triển an ninh mạng bao gồm: a) Xây dựng hệ thống phần mềm, trang thiết bị bảo vệ an ninh mạng; b) Phương pháp thẩm định phần mềm, trang thiết bị bảo vệ an ninh mạng đạt chuẩn và hạn chế tồn tại điểm yếu, lỗ hổng bảo mật, phần mềm độc hại; c) Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng; d) Phương pháp bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; khả năng bảo mật khi truyền đưa thông tin trên không gian mạng; đ) Xác định nguồn gốc của thông tin được truyền đưa trên không gian mạng;	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	đ) Xác định nguồn gốc của thông tin được truyền đưa trên không gian mạng; e) Giải quyết nguy cơ đe dọa an ninh mạng; g) Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng; h) Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng; i) Dự báo an ninh mạng; k) Nghiên cứu thực tiễn, phát triển lý luận an ninh mạng. 2. Cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.		e) Giải quyết nguy cơ đe dọa an ninh mạng; g) Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng; h) Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng; i) Dự báo an ninh mạng; k) Nghiên cứu thực tiễn, phát triển lý luận an ninh mạng. 2. Cơ quan, tổ chức, cá nhân có liên quan có quyền nghiên cứu, phát triển an ninh mạng.	
46.	**Điều 28. Nâng cao năng lực tự chủ về an ninh mạng** 1. Nhà nước khuyến khích, tạo điều kiện để cơ quan, tổ chức, cá nhân nâng cao năng lực tự chủ về an ninh mạng và nâng cao khả năng sản xuất, kiểm tra, đánh giá, kiểm định thiết bị số, dịch vụ mạng, ứng dụng mạng. 2. Chính phủ thực hiện các biện pháp sau đây để nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân: a) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng;		Điều 46. Nâng cao năng lực tự chủ về an ninh mạng 1. Nhà nước khuyến khích, tạo điều kiện để cơ quan, tổ chức, cá nhân nâng cao năng lực tự chủ về an ninh mạng và nâng cao khả năng sản xuất, kiểm tra, đánh giá, kiểm định thiết bị số, dịch vụ mạng, ứng dụng mạng. 2. Chính phủ thực hiện các biện pháp sau đây để nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân: a) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng; b) Thúc đẩy ứng dụng công nghệ mới,	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	b) Thúc đẩy ứng dụng công nghệ mới, công nghệ tiên tiến liên quan đến an ninh mạng; c) Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng; d) Tăng cường môi trường kinh doanh, cải thiện điều kiện cạnh tranh hỗ trợ doanh nghiệp nghiên cứu, sản xuất sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng.		công nghệ tiên tiến liên quan đến an ninh mạng; c) Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng; d) Tăng cường môi trường kinh doanh, cải thiện điều kiện cạnh tranh hỗ trợ doanh nghiệp nghiên cứu, sản xuất sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng.	
47.	**Điều 30. Lực lượng bảo vệ an ninh mạng** 1. Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng. 2. Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia. 3. Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.		Điều 47. Lực lượng chuyên trách bảo vệ an ninh mạng 1. Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng. 2. Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia. 3. Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018
48.	**Điều 31. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng** 1. Công dân Việt Nam có kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin là nguồn lực cơ bản, chủ yếu bảo vệ an ninh mạng. 2. Nhà nước có chương trình, kế		Điều 48. Bảo đảm nguồn nhân lực bảo vệ an ninh mạng 1. Công dân Việt Nam có kiến thức về an ninh mạng, công nghệ thông tin là nguồn lực cơ bản, chủ yếu bảo vệ an ninh mạng. 2. Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng. 3. Khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc nguy cơ đe dọa an ninh mạng, cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng. Thẩm quyền, trách nhiệm, trình tự, thủ tục huy động nhân lực bảo vệ an ninh mạng được thực hiện theo quy định của Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và quy định khác của pháp luật có liên quan.		bảo vệ an ninh mạng. 3. Khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc nguy cơ đe dọa an ninh mạng, cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng. Thẩm quyền, trách nhiệm, trình tự, thủ tục huy động nhân lực bảo vệ an ninh mạng được thực hiện theo quy định của Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và quy định khác của pháp luật có liên quan.	
49.	**Điều 32. Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng** 1. Công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng. 2. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao. 3. Ưu tiên phát triển cơ sở đào		Điều 49. Tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng 1. Công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng. 2. Ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao. 3. Ưu tiên phát triển cơ sở đào tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà nước và khu vực tư nhân, trong nước và ngoài nước.		nước và khu vực tư nhân, trong nước và nước ngoài.	
50.	**Điều 33. Giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng** 1. Nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường, chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh. 2. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng. Bộ Quốc phòng, Ban Cơ yếu Chính phủ tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý.		Điều 50. Giáo dục bồi dưỡng kiến thức, nghiệp vụ an ninh mạng 1. Nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường, chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh. 2. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng. Bộ Quốc phòng tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho đối tượng thuộc phạm vi quản lý.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018
51.	**Điều 34. Phổ biến kiến thức về an ninh mạng** 1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến		Điều 51. Phổ biến kiến thức về an ninh mạng 1. Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà	

	khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng. 2. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức. 3. Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.		nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng. 2. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong Bộ, ngành, cơ quan, tổ chức. 3. Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018
52.			Điều 52. Yêu cầu về kiến thức, kỹ năng bảo đảm an ninh mạng đối với người đứng đầu, lãnh đạo cơ quan, tổ chức, doanh nghiệp nhà nước, lực lượng chuyên trách bảo vệ an ninh mạng và cán bộ phụ trách bảo vệ an ninh mạng 1. Thủ trưởng cơ quan và cấp phó phụ trách bảo đảm an ninh mạng của các cơ quan nhà nước, doanh nghiệp nhà nước, tổ chức kinh tế nhà nước và cơ quan chủ quản hệ thống thông tin quan trọng quốc gia đáp ứng yêu cầu kiến thức, kỹ năng về bảo đảm an ninh mạng, được cơ quan có thẩm quyền chứng nhận theo quy định.	BỔ SUNG MỚI

			2. Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ; lực lượng bảo vệ an ninh mạng tại các Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng quốc gia phải đáp ứng yêu cầu kiến thức, kỹ năng về bảo đảm an ninh mạng. 3. Cán bộ, chuyên gia chịu trách nhiệm về bảo đảm an ninh mạng trong cơ quan, tổ chức, doanh nghiệp Nhà nước phải tham gia sát hạch và được cấp chứng chỉ kiến thức, kỹ năng về bảo đảm an ninh mạng. 2. Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan tổ chức triển khai đánh giá, xác nhận đạt yêu cầu và cấp chứng chỉ kiến thức, kỹ năng về bảo đảm an ninh mạng thông qua chương trình bồi dưỡng, sát hạch và cấp chứng chỉ theo từng đối tượng liên quan. 3. Kết quả hoàn thành chương trình bồi dưỡng và chứng chỉ về bảo đảm an ninh mạng được sử dụng làm căn cứ để xem xét bổ nhiệm, bổ nhiệm lại, quy hoạch cán bộ và đánh giá năng lực trong lĩnh vực công tác có liên quan đến an ninh mạng. 4. Chính phủ quy định chi tiết chuẩn kiến thức, nội dung chương trình bồi dưỡng, thẩm quyền sát hạch, cấp chứng chỉ và lộ trình áp dụng đối với	

			từng nhóm chức danh lãnh đạo và đối tượng liên quan	
53.	**Điều 35. Kinh phí bảo vệ an ninh mạng** 1. Kinh phí bảo vệ an ninh mạng của cơ quan nhà nước, tổ chức chính trị do ngân sách nhà nước bảo đảm, được bố trí trong dự toán ngân sách nhà nước hằng năm. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật về ngân sách nhà nước. 2. Kinh phí bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan, tổ chức ngoài quy định tại khoản 1 Điều này do cơ quan, tổ chức tự bảo đảm.		Điều 53. Kinh phí bảo vệ an ninh mạng 1. Kinh phí bảo vệ an ninh mạng của cơ quan nhà nước, tổ chức chính trị do ngân sách nhà nước bảo đảm, được bố trí trong dự toán ngân sách nhà nước hằng năm. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật về ngân sách nhà nước. 2. Kinh phí bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan, tổ chức ngoài quy định tại khoản 1 Điều này do cơ quan, tổ chức tự bảo đảm.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018
54.		**Điều 52. Trách nhiệm quản lý nhà nước về an toàn thông tin mạng** 1. Chính phủ thống nhất quản lý nhà nước về an toàn thông tin mạng. 2. Bộ Thông tin và Truyền thông chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an toàn thông tin mạng, có nhiệm vụ, quyền hạn sau đây: a) Ban hành hoặc xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật, chiến lược, quy hoạch, kế hoạch, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng;	Điều 54. Quản lý nhà nước về an ninh mạng 1. Nội dung quản lý nhà nước về an ninh mạng bao gồm: a) Xây dựng chủ trương, chính sách, chiến lược, quy hoạch, kế hoạch, chương trình trong lĩnh vực an ninh mạng. b) Ban hành và tổ chức thực hiện văn bản quy phạm pháp luật về an ninh mạng; xây dựng, ban hành tiêu chuẩn quy chuẩn kỹ thuật an ninh mạng. c) Quản lý hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng. d) Quản lý công tác đánh giá, công bố	KẾ THỪA LUẬT AN TOÀN THÔNG TIN MẠNG NĂM 2015 (SỬA ĐỔI, BỔ SUNG NĂM 2018),

		b) Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin; c) Quản lý công tác giám sát an toàn hệ thống thông tin trên toàn quốc, trừ hệ thống thông tin quy định tại điểm c khoản 3 và điểm b khoản 5 Điều này; d) Quản lý công tác đánh giá về an toàn thông tin mạng; đ) Cấp Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, Giấy phép nhập khẩu sản phẩm an toàn thông tin, trừ sản phẩm, dịch vụ mật mã dân sự; e) Nghiên cứu, ứng dụng khoa học và công nghệ về an toàn thông tin mạng; đào tạo, bồi dưỡng, phát triển nguồn nhân lực; g) Quản lý và thực hiện hợp tác quốc tế về an toàn thông tin mạng; h) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an toàn thông tin mạng; i) Chủ trì, phối hợp với bộ, ngành, Ủy ban nhân dân cấp tỉnh và doanh nghiệp có liên quan trong việc bảo đảm an toàn thông tin mạng; k) Tổ chức tuyên truyền, phổ biến pháp luật về an toàn thông tin mạng; l) Định kỳ hằng năm báo cáo Chính phủ về hoạt động an toàn thông tin mạng. 3. Bộ Quốc phòng có nhiệm vụ,	hợp chuẩn, hợp quy về an ninh mạng. e) Quản lý công tác giám sát an ninh mạng. f) Thẩm định về an ninh mạng trong hồ sơ thiết kế hệ thống thông tin. g) Tuyên truyền, phổ biến pháp luật về an ninh mạng. h) Tổ chức nghiên cứu, ứng dụng khoa học và công nghệ về an ninh mạng; phát triển nguồn nhân lực an ninh mạng; đào tạo về an ninh mạng. i) Phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, tội phạm sử dụng công nghệ cao. k) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo, xử lý vi phạm pháp luật về an ninh mạng. l)Hợp tác quốc tế về an ninh mạng. 2. Trách nhiệm quản lý nhà nước về an ninh mạng a) Chính phủ thống nhất quản lý nhà nước về an ninh mạng. b) Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện thống nhất quản lý nhà nước về an ninh mạng trên phạm vi toàn quốc, trừ quy định tại khoản 3 Điều này. c) Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng thuộc phạm vi quản lý. Ban Cơ yếu Chính phủ chịu trách nhiệm trước Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về	

		quyền hạn sau đây: a) Ban hành hoặc xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật, chiến lược, quy hoạch, kế hoạch, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng thuộc lĩnh vực do Bộ Quốc phòng quản lý; b) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật trong hoạt động bảo đảm an toàn thông tin mạng thuộc lĩnh vực do Bộ Quốc phòng quản lý; c) Thực hiện quản lý công tác giám sát an toàn hệ thống thông tin thuộc Bộ Quốc phòng. 4. Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng thực hiện quản lý nhà nước về mật mã dân sự, có nhiệm vụ sau đây: a) Xây dựng, trình cấp có thẩm quyền ban hành văn bản quy phạm pháp luật về quản lý mật mã dân sự; b) Chủ trì, phối hợp với bộ, ngành có liên quan xây dựng, trình cơ quan nhà nước có thẩm quyền ban hành tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia đối với sản phẩm, dịch vụ mật mã dân sự; c) Quản lý hoạt động kinh doanh, sử dụng mật mã dân sự; quản lý chất lượng sản phẩm, dịch vụ mật mã dân sự; quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy đối với sản	mật mã dân sự và an ninh mạng thuộc phạm vi quản lý theo quy định của pháp luật về cơ yếu. d) Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình thực hiện công tác bảo vệ an ninh mạng; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng; e) Ủy ban nhân dân cấp tỉnh thực hiện công tác bảo vệ an ninh mạng và quản lý nhà nước về dữ liệu tại địa phương.	

		phẩm, dịch vụ mật mã dân sự; d) Xây dựng, trình cấp có thẩm quyền ban hành Danh mục sản phẩm, dịch vụ mật mã dân sự và Danh mục sản phẩm mật mã dân sự xuất khẩu, nhập khẩu theo giấy phép; đ) Cấp Giấy phép kinh doanh sản phẩm, dịch vụ mật mã dân sự, Giấy phép xuất khẩu, nhập khẩu sản phẩm mật mã dân sự; e) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật trong hoạt động kinh doanh, sử dụng mật mã dân sự; g) Hợp tác quốc tế về mật mã dân sự. 5. Bộ Công an có nhiệm vụ, quyền hạn sau đây: a) Chủ trì, phối hợp với bộ, ngành có liên quan xây dựng và trình cấp có thẩm quyền ban hành hoặc ban hành theo thẩm quyền và hướng dẫn thực hiện văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước, phòng, chống tội phạm mạng, lợi dụng mạng để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội; b) Thực hiện quản lý công tác giám sát an toàn hệ thống thông tin thuộc Bộ Công an; c) Tổ chức, chỉ đạo, triển khai công tác phòng, chống tội phạm, tổ chức điều tra tội phạm mạng và hành vi vi		

		phạm pháp luật khác trong lĩnh vực an toàn thông tin mạng; d) Phối hợp với Bộ Thông tin và Truyền thông, bộ, ngành có liên quan kiểm tra, thanh tra về an toàn thông tin mạng, xử lý vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền. 6. Bộ Nội vụ có trách nhiệm tổ chức đào tạo, bồi dưỡng kiến thức, nghiệp vụ an toàn thông tin mạng cho cán bộ, công chức, viên chức. 7. Bộ Giáo dục và Đào tạo có trách nhiệm tổ chức đào tạo, phổ biến kiến thức về an toàn thông tin mạng trong cơ sở giáo dục đại học. 8. Bộ Lao động - Thương binh và Xã hội có trách nhiệm tổ chức đào tạo, bồi dưỡng, phổ biến kiến thức về an toàn thông tin mạng trong cơ sở giáo dục nghề nghiệp. 9. Bộ Tài chính có trách nhiệm hướng dẫn, bố trí kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng theo quy định của pháp luật. 10. Bộ, cơ quan ngang bộ trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm quản lý an toàn thông tin mạng của ngành mình và phối hợp với Bộ Thông tin và Truyền thông thực hiện quản lý nhà nước về an toàn thông tin mạng. 11. Ủy ban nhân dân cấp tỉnh trong phạm vi nhiệm vụ, quyền hạn của		

		mình thực hiện quản lý nhà nước về an toàn thông tin mạng ở địa phương. **Điều 51. Nội dung quản lý nhà nước về an toàn thông tin mạng** 1. Xây dựng chiến lược, quy hoạch, kế hoạch và chính sách trong lĩnh vực an toàn thông tin mạng; xây dựng và chỉ đạo thực hiện chương trình quốc gia về an toàn thông tin mạng. 2. Ban hành và tổ chức thực hiện văn bản quy phạm pháp luật về an toàn thông tin mạng; xây dựng, công bố tiêu chuẩn quốc gia, ban hành quy chuẩn kỹ thuật về an toàn thông tin mạng. 3. Quản lý nhà nước về mật mã dân sự. 4. Quản lý công tác đánh giá, công bố hợp chuẩn, hợp quy về an toàn thông tin mạng. 5. Quản lý công tác giám sát an toàn hệ thống thông tin. 6. Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin. 7. Tuyên truyền, phổ biến pháp luật về an toàn thông tin mạng. 8. Quản lý hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng. 9. Tổ chức nghiên cứu, ứng dụng khoa học và công nghệ về an toàn		

		thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; đào tạo cán bộ chuyên trách về an toàn thông tin mạng. 10. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo, xử lý vi phạm pháp luật về an toàn thông tin mạng. 11. Hợp tác quốc tế về an toàn thông tin mạng.		
55.	Điều 36. Trách nhiệm của Bộ Công an Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng và có nhiệm vụ, quyền hạn sau đây, trừ nội dung thuộc trách nhiệm của Bộ Quốc phòng và Ban Cơ yếu Chính phủ: 1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng; 2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; 3. Phòng ngừa, đấu tranh với hoạt động sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm mạng; 4. Bảo đảm an ninh thông tin		Điều 55. Trách nhiệm của Bộ Công an Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng và có nhiệm vụ, quyền hạn sau đây, trừ nội dung thuộc trách nhiệm của Bộ Quốc phòng: 1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng; 2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; 3. Phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam quy định tại khoản 1 Điều 20 của Luật này. 4. Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về an ninh mạng trên dịch vụ, hệ thống thông tin do	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	trên không gian mạng; xây dựng cơ chế xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin an ninh mạng, nguy cơ đe dọa an ninh mạng; 5. Tham mưu, đề xuất Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều Bộ, ngành; 6. Tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; 7. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng. Điều 38. Trách nhiệm của Bộ Thông tin và Truyền thông 1. Phối hợp với Bộ Công an, Bộ Quốc phòng trong bảo vệ an ninh mạng. 2. Phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ		doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý. 5. 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; 6. Bảo đảm an ninh thông tin trên không gian mạng, an ninh dữ liệu; xây dựng cơ chế xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin an ninh mạng, nguy cơ đe dọa an ninh mạng; 7. Tham mưu, đề xuất Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều Bộ, ngành; 8. Tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; 9. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng, an ninh thông tin, an ninh dữ liệu.	

	nghĩa Việt Nam quy định tại khoản 1 Điều 16 của Luật này. 3. Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về an ninh mạng trên dịch vụ, hệ thống thông tin do doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý.			
56.	Điều 37. Trách nhiệm của Bộ Quốc phòng Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng trong phạm vi quản lý và có nhiệm vụ, quyền hạn sau đây: 1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý; 2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong phạm vi quản lý; 3. Phòng ngừa, đấu tranh với các hoạt động sử dụng không		Điều 56. Trách nhiệm của Bộ Quốc phòng Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng trong phạm vi quản lý và có nhiệm vụ, quyền hạn sau đây: 1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý; 2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong phạm vi quản lý; 3. Phòng ngừa, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia trong phạm vi quản lý; 4. Phối hợp với Bộ Công an tổ chức diễn tập phòng, chống tấn công mạng,	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	gian mạng xâm phạm an ninh quốc gia trong phạm vi quản lý; 4. Phối hợp với Bộ Công an tổ chức diễn tập phòng, chống tấn công mạng, diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, triển khai thực hiện công tác bảo vệ an ninh mạng; 5. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng trong phạm vi quản lý.		diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, triển khai thực hiện công tác bảo vệ an ninh mạng; 5. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng trong phạm vi quản lý.	
57.	Điều 39. Trách nhiệm của Ban Cơ yếu Chính phủ 1. Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ an ninh mạng thuộc phạm vi Ban Cơ yếu Chính phủ quản lý. 2. Bảo vệ an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp theo quy định của Luật này. 3. Thống nhất quản lý nghiên cứu khoa học, công nghệ mật mã; sản xuất, sử dụng, cung cấp		Điều 57. Trách nhiệm của Ban Cơ yếu Chính phủ 1. Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ an ninh mạng thuộc phạm vi Ban Cơ yếu Chính phủ quản lý. 2. Bảo vệ an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp theo quy định của Luật này. 3. Thống nhất quản lý nghiên cứu khoa học, công nghệ mật mã; sản xuất, sử dụng, cung cấp sản phẩm mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	sản phẩm mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.			
58.	Điều 40. Trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh Trong phạm vi nhiệm vụ, quyền hạn của mình, Bộ, ngành, Ủy ban nhân dân cấp tỉnh có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin thuộc phạm vi quản lý; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng của Bộ, ngành, địa phương.		Điều 58. Trách nhiệm của Bộ, ngành, Ủy ban nhân dân các cấp Trong phạm vi nhiệm vụ, quyền hạn của mình, Bộ, ngành, Ủy ban nhân các cấp có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin thuộc phạm vi quản lý; phối hợp với lực lượng Công an nhân dân cấp tương ứng thực hiện quản lý nhà nước về an ninh mạng của Bộ, ngành, địa phương.	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018
59.			Điều 59. Trách nhiệm của chủ quản hệ thống thông tin trong bảo vệ an ninh mạng 1. Chủ quản hệ thống thông tin có trách nhiệm thực hiện bảo vệ hệ thống thông tin theo quy định tại Luật này. 2. Kết nối hệ thống giám sát an ninh mạng, hệ thống phòng chống mã độc tập trung về Trung tâm An ninh mạng quốc gia của Bộ Công an hoặc Trung tâm An ninh mạng của tỉnh để hỗ trợ giám sát an ninh mạng. 3. Báo cáo sự cố an ninh mạng với cơ quan chuyên trách của Bộ Công an hoặc Bộ Quốc phòng. 2. Chủ quản hệ thống thông tin sử dụng ngân sách nhà nước thực hiện	BỔ SUNG MỚI

			trách nhiệm quy định tại khoản 1 Điều này và có trách nhiệm sau đây: a) Có phương án bảo đảm an ninh mạng được cơ quan nhà nước có thẩm quyền thẩm định khi thiết lập, mở rộng hoặc nâng cấp hệ thống thông tin; b) Chỉ định cá nhân, bộ phận phụ trách về an ninh mạng.	
60.	Điều 41. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng 1. Doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm sau đây: a) Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa; b) Xây dựng phương án, giải pháp phản ứng nhanh với sự cố an ninh mạng, xử lý ngay điểm yếu, lỗ hổng bảo mật, mã độc, tấn công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này;		Điều 60. Trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng 1. Tuân thủ quy định của pháp luật về an ninh mạng. 2. Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa. 3. Xây dựng phương án, giải pháp phản ứng nhanh với sự cố an ninh mạng, xử lý ngay điểm yếu, lỗ hổng bảo mật, mã độc, tấn công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này. 4. Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	c) Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp 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 đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này; d) Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong bảo vệ an ninh mạng. 2. Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm thực hiện quy định tại khoản 1 Điều này, khoản 2 và khoản 3 Điều 26 của Luật này.		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 đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này; 5. Thực hiện theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để quản lý định danh IP. 6. Phối hợp, thực hiện theo yêu cầu, hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để thiết lập hệ thống kết nối, đấu nối đường truyền kỹ thuật, truyền tải dữ liệu và đáp ứng các điều kiện cần thiết khác để triển khai các giải pháp, biện pháp bảo vệ an ninh mạng. 7. Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm thực hiện quy định tại Điều này, khoản 2 và khoản 3 Điều 36 của Luật này.	
61.	Điều 42. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng 1. Tuân thủ quy định của pháp luật về an ninh mạng. 2. Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh		Điều 61. Trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng 1. Tuân thủ quy định của pháp luật về an ninh mạng. 2. Có trách nhiệm bảo mật thông tin đăng ký, mở, quản lý, sử dụng tài	- KẾ THỪA LUẬT AN NINH MẠNG NĂM 2018

	mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng. 3. Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.		khoản số của mình; trường hợp tài khoản số được sử dụng để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ vi phạm, chủ tài khoản bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường thiệt hại theo quy định pháp luật. 3. Cung cấp thông tin, tài liệu cho cơ quan có thẩm quyền, nhà cung cấp dịch vụ trung thực, đầy đủ theo quy định pháp luật. 4. Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng.	
62.			Điều 62. Điều khoản chuyển tiếp 1. Các cơ quan, tổ chức, cá nhân có trách nhiệm hoàn thành việc chuyển đổi các nội dung liên quan từ Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) sang tuân thủ theo quy định của Luật An ninh mạng năm 2025 trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành. Trong thời gian chưa hoàn thành việc chuyển đổi, các cơ quan, tổ chức, cá nhân tiếp tục áp dụng các quy định của Luật An toàn thông tin mạng không trái với quy định của Luật này. 2. Đối với các hồ sơ hệ thống thông tin đã có Quyết định công nhận cấp độ	HỢP NHẤT

			trước khi Luật này có hiệu lực thì không cần hoàn thiện hồ sơ theo quy định cấp độ mới, nhưng áp dụng các điều kiện, tiêu chuẩn, biện pháp bảo vệ tương ứng với quy định cấp độ mới trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành. 3. Đối với hệ thống thông tin quan trọng về an ninh quốc gia đã đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành: a) Chủ quản hệ thống thông tin có trách nhiệm rà soát, đánh giá và thực hiện các biện pháp bảo đảm an ninh mạng theo quy định của Luật này; b) Trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành, chủ quản hệ thống thông tin phải hoàn thành việc đánh giá điều kiện an ninh mạng và thẩm định an ninh mạng theo quy định của Luật này. 4. Các phương án, quy trình, thủ tục bảo đảm an toàn thông tin được ban hành theo Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018) phải được rà soát, điều chỉnh, bổ sung cho phù hợp với các quy định của Luật này trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành. 5. Các sản phẩm, dịch vụ, giải pháp, phương tiện kỹ thuật bảo đảm an toàn thông tin mạng đã được đưa vào sử dụng trước ngày Luật này có hiệu lực thi hành, nếu không đáp ứng các điều	

			kiện an ninh mạng theo quy định của Luật này thì phải được thay thế hoặc nâng cấp trong thời hạn 12 tháng kể từ ngày Luật này có hiệu lực thi hành. 6. Chính phủ quy định chi tiết việc thực hiện các điều khoản chuyển tiếp quy định tại Điều này. 7. Văn bản quy phạm pháp luật có sử dụng thuật ngữ "an toàn thông tin mạng", "an toàn, an ninh mạng" được thay thế bằng cụm từ "an ninh mạng" kẻ từ ngày luật này có hiệu lực thi hành.	
63.			Điều 63. Hiệu lực thi hành 1. Luật này có hiệu lực th hành từ ngày 01 tháng 01 năm 2026. 2. Luật An toàn thông tin mạng số 86/2015/QH13, ban hành ngày 19 tháng 11 năm 2015, đã được sửa đổi, bổ sung một số điều và hợp nhất theo Luật số 29/VBHN/VPQH, ngày 10 tháng 12 năm 2018 và Luật An ninh mạng số 24/2018/QH14, ngày 12 tháng 6 năm 2018 hết hiệu lực kể từ ngày Luật này có hiệu lự c thi hành, trừ các quy định tại Điều 61 của Luật này.	HỢP NHẤT