TÌM HIỂU LUẬT AN NINH MẠNG

Câu 1. Vì sao phải ban hành Luật an ninh mạng?

Trả lời:

Việc ban hành Luật an ninh mạng để đáp ứng yêu cầu cấp thiết về bảo vệ an ninh mạng trong tình hình hiện nay, vì:

- Nước ta đang phải đối phó với hàng chục ngàn cuộc tấn công mạng với quy mô lớn, cường độ cao mỗi năm, đe dọa trực tiếp đến an ninh quốc gia và trật tự an toàn xã hội, gây tổn hại nặng nề về kinh tế.

- Không gian mạng và một số loại hình dịch vụ, ứng dụng trên không gian mạng đang bị các thế lực thù địch, phản động sử dụng để tán phát thông tin kêu gọi biểu tình, tụ tập trái phép phá rối an ninh trật tự, kích động bạo loạn, khủng bố, lật đổ chính quyền nhân dân, xâm phạm chủ quyền, lợi ích, an ninh quốc gia.

- Tình trạng đăng thông tin xuyên tạc chủ trương, đường lối của Đảng, Nhà nước, phá hoại khối đại đoàn kết dân tộc; lan truyền thông tin sai sự thật, vu khống tổ chức, cá nhân… diễn ra tràn lan trên không gian mạng nhưng chưa có biện pháp quản lý hữu hiệu, dẫn tới nhiều hậu quả nghiêm trọng về tính mạng con người, tinh thần, kinh tế, tệ nạn xã hội.

- Năng lực, tiềm lực quốc gia về an ninh mạng chưa có chính sách điều chỉnh phù hợp, kịp thời; sự phụ thuộc vào thiết bị công nghệ thông tin có nguồn gốc nước ngoài; … đặt yêu cầu bức thiết phải xây dựng, hình thành nền công nghiệp an ninh mạng.

- Công tác quản lý nhà nước về an ninh thông tin, an ninh mạng tại các bộ, ban, ngành, địa phương còn tồn tại những bất cập, hạn chế, thiếu đồng bộ do chưa có văn bản quy phạm pháp luật nào điều chỉnh vấn đề này.

Thực trạng, nguy cơ trên đã đặt ra yêu cầu bức thiết phải xây dựng và ban hành văn bản luật về an ninh mạng để phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Câu 2. Luật an ninh mạng có chính sách ưu tiên, tạo điều kiện cho các cơ quan, doanh nghiệp, tổ chức, cá nhân trong lĩnh vực này hay không?

Trả lời: Luật an ninh mạng quy định 05 chính sách lớn của Nhà nước trong lĩnh vực an ninh mạng bao gồm:

- 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.

- 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.

- 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.

- 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 các cơ quan chức năng trong bảo vệ an ninh mạng.

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

Câu 3. Luật an ninh mạng có bảo vệ quyền con người không?

Trả lời:

Luật an ninh mạng bảo vệ quyền con người khi tham gia hoạt động trên không gian mạng. Đồng thời, Luật an ninh mạng phù hợp với tinh thần của Hiến chương Liên hợp quốc, Tuyên ngôn về quyền con người của Đại hội đồng Liên hợp quốc (1948) và các văn bản khác có liên quan, phù hợp với Hiến pháp năm 2013 của nước Cộng xã hội chủ nghĩa Việt Nam, Bộ luật hình sự, Bộ luật dân sự Việt Nam.

Luật an ninh mạng trực tiếp bảo vệ 05 quyền con người sau đây:

- Quyền sống, quyền tự do và an ninh cá nhân; quyền bình đẳng trước pháp luật và được pháp luật bảo vệj;

- Quyền không bị can thiệp vào đời tư, gia đình, chỗ ở hoặc thư tín;

- Quyền không bị xâm hại danh dự hay uy tín cá nhân;

- Quyền tự do tư tưởng, tín ngưỡng và tôn giáo của công dân;

- Quyền tự do ngôn luận, tự do biểu đạt của công dân.

Câu 4. Luật an ninh mạng có ngăn cản, xâm phạm quyền tự do ngôn luận không?

Trả lời:

Luật an ninh mạng không ngăn cản, xâm phạm quyền tự do ngôn luận của công dân. Các hoạt động liên lạc, trao đổi, đăng tải, chia sẻ thông tin, mua bán, kinh doanh, thương mại vẫn diễn ra bình thường trên không gian mạng, không hề bị ngăn cản, cấm đoán miễn là những hoạt động đó không vi phạm pháp luật của Việt Nam.

Công dân có thể làm bất cứ điều gì trên không gian mạng mà pháp luật Việt Nam không cấm. Đồng thời, Luật an ninh mạng bảo vệ cho các hoạt động tự do ngôn luận, quyền và lợi ích hợp pháp của tổ chức cá nhân khi mua bán, kinh doanh, trao đổi, thương mại trên không gian mạng.

Câu 5. Luật an ninh mạng có cấm người sử dụng Internet truy cập Facebook, Google, Youtube không?

Trả lời: Không

Luật an ninh mạng không cấm người dân truy cập Facebook, Google, Youtube. Người dân Việt Nam vẫn được tự do truy cập vào các trang mạng của Facebook, Google, Youtube hay bất kỳ trang mạng xã hội nào khác ở trong nước hay nước ngoài. Ngược lại, Luật an ninh mạng quy định các biện pháp bảo vệ về an ninh mạng cho người dân khi tham gia hoạt động trên các trang mạnh xã hội Facebook, Google, Youtube,…

Tuy nhiên, người nào sử dụng những mạng xã hội trên hoặc bất kỳ mạng xã hội nào khác để thực hiện hành vi vi phạm pháp luật đều bị xử lý nghiêm theo quy định của pháp luật.

Câu 6. Luật an ninh mạng có làm lộ thông tin cá nhân của người sử dụng không?

Trả lời:

Thông tin cá nhân được Luật an ninh mạng bảo vệ chặt chẽ. Các cơ quan chức năng, doanh nghiệp và tổ chức, cá nhân có liên quan phải chịu trách nhiệm bảo vệ bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng.

Các hành vi như chiếm đoạt, mua bán, thu giữ, cố ý làm lộ, xóa, làm hư hỏng, thất lạc, thay đổi, đưa lên không gian mạng những thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư của người khác mà chưa được phép của người sử dụng hoặc trái quy định của pháp luật sẽ bị xử lý. Đồng thời, lực lượng chuyên trách bảo vệ an ninh mạng nếu lạm dụng, làm lộ thông tin cá nhân của người sử dụng sẽ bị xử lý theo quy định của pháp luật.

Câu 7. Cá nhân có quyền lợi gì theo quy định của Luật an ninh mạng?

Trả lời:

- Được bảo vệ khi tham gia hoạt động trên không gian mạng trước các thông tin xấu độc xâm phạm tới danh dự, uy tín, nhân phẩm, các hoạt động tấn công mạng, gián điệp mạng, khủng bố mạng hoặc các hành vi khác gây ảnh hưởng tới quyền và lợi ích hợp pháp của mình.

- Được tham gia, thừa hưởng các chính sách về an ninh mạng của Nhà nước như: nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; giao dục, bồi dưỡng kiến thức an ninh mạng.

- Được trao công cụ để bảo vệ quyền lợi của mình với các quy định tại Điều 16 (xử lý thông tin trên không gian mạng vi phạm pháp luật), Điều 17 (bảo vệ người dân trước các hoạt động gián điệp mạng, bảo vệ bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng), Điều 18 (bảo vệ người dân khỏi các hoạt động tội phạm mạng, như chiếm đoạt tài sản, trộm cắp thông tin

thẻ tín dụng, tài khoản ngân hàng...), Điều 19 (bảo vệ người dân khỏi hoạt động tấn công mạng như tán phát mã độc, tấn công từ chối dịch vụ,…)

- Trẻ em được bảo vệ đặc biệt trên không gian mạng theo quy định tại Điều 29 Luật an ninh mạng *(Nội dung chi tiết xem tại Câu số 26 Phần II)*. Đây là quy định tiến bộ, phù hợp với thực tế hiện nay.

Câu 8. Cá nhân có trách nhiệm gì theo quy định của Luật an ninh mạng?

Trả lời: Cá nhân có trách nhiệm sau đây:

- Không thực hiện các hành vi bị nghiêm cấm được quy định tại Điều 8 Luật an ninh mạng.

- Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan quản lý nhà nước có thẩm quyền, lực lượng bảo vệ an ninh mạng.

- Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạnh trong phòng ngừa, xử lý các hành vi sử dụng không gian mạng vi phạm pháp luật.

Câu 9. Doanh nghiệp có quyền lợi gì theo quy định của Luật an ninh mạng?

Trả lời:

- Được bảo vệ tốt hơn trước các hành vi vi phạm pháp luật trên không gian mạng như tung tin thất thiệt về sản phẩm, dịch vụ, canh tranh không lành mạnh, xâm phạm sở hữu trí tuệ, bí mật kinh doanh, chiếm đoạt tài sản, tấn công từ chối dịch vụ…

- Bình đẳng với các doanh nghiệp nước ngoài về thủ tục pháp lý, từ đăng ký kinh doanh, xin cấp phép dịch vụ, thanh tra, kiểm tra, thuế, có điều kiện canhjt ranh công bằng, chống độc quyền, thao túng giá.

- Cơ hội phát triển cho các doanh nghiệp công nghệ thông tin, viễn thông và an ninh mạng khi Luật an ninh mạng hướng đến xây dựng nền công nghệ an ninh mạng tự chủ, sáng tạo. Do đó, đây là điều kiện thuận lợi và rất rõ rang cho các doanh nghiệp trong nước phát triển.

Câu 10. Doanh nghiệp có trách nhiệm gì theo quy định của Luật an ninh mạng?

Trả lời:

- Không vi phạm các hành vi bị nghiêm cấm tại Điều 8 Luật an ninh mạng.

- Phối hợp với các cơ quan chức năng có thẩm quyền về an ninh mạng xử lý thông tin và hành vi vi phạm pháp luật, trong đó có xử lý tình huống nguy hiểm về an ninh mạng, bảo vệ trẻ em trên không gian mạng;

- Lưu trữ một số loại dữ liệu theo quy định của Chính phủ.

Câu 11. Các khái niệm "An ninh mạng", "Bảo vệ an ninh mạng", "Không gian mạng", "Không gian mạng quốc gia", "Tội phạm mạng", "Tấn công mạng", "Khủng bố mạng", "Gián điệp mạng", "Nguy cơ đe dọa an ninh mạng", "Sự cố an ninh mạng", "Tình huống nguy hiểm về an ninh mạng" được hiểu như thế nào?

Trả lời:

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

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.

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

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.

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.

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.

Gián điệp mạng là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của cơ quan, tổ chức, cá nhân.

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.

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.

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.

Câu 12: Nguyên tắc bảo vệ an ninh mạng là gì?

Trả lời:

Điều 4 Luật an ninh mạng quy định nguyên tắc bảo vệ an ninh mạng như sau:

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

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

Câu 13. Luật an ninh mạng nghiêm cấm những hành vi nào?

Trả lời: Điều 8 Luật an ninh mạng nghiêm cấm các hành vi sau:

1. 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:

Đăng tải, phát tán 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. Thông tin có nội dung làm nhục, vu khống; Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế. 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.

Thực hiện các 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: 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 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. 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; 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. Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại. 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).

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;

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;

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

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

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.

- 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;

- 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;

- 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;

- 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;

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

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

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

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

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

6. Hành vi khác vi phạm quy định của Luật an ninh mạng.

Câu 14. 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 được quy định như thế nào?

Trả lời:

- Thông tin trên không gian mạng có nội dung 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.

- 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:

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.

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

Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

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.

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

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.

Câu 15. 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 được quy định như thế nào?

Trả lời: Những hành vi sau đây là 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:

- 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 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;

- 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;

- 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;

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

- 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.

Câu 16. Trách nhiệm của Chủ quản hệ thống thông tin trong phòng, chống 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?

Trả lời:

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

- 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;

- 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;

- 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.

Câu 17. Luật an ninh mạng quy định như thế nào về 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?

Trả lời:

- 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:

Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4, 5 Điều 16 và khoản 1 Điều 17 của Luật an ninh mạng.

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;

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;

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

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

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.

- 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.

Câu 18. Hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng được quy định như thế nào?

Trả lời:

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

- 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;

- 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;

- 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;

- 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;

- 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;

- 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.

Câu 19. Tình huống nguy hiểm về an ninh mạng được quy định như thế nào ?

Trả lời:

Điều 21 Luật an ninh mạng quy định tình huống nguy hiểm về an ninh mạng bao gồm:

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

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

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

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

- 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.

Câu 20. Đấu tranh bảo vệ an ninh mạng là gì? Nội dung của đấu tranh bảo vệ an ninh mạng quy định như thế nào?

Trả lời:

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.

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

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

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

- 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;

- 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.

Câu 21. Nội dung triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương được quy định như thế nào?

Trả lời:

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

- 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;

- 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;

- 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;

- 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;

- 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;

- 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.

Câu 22. Nội dung nghiên cứu, phát triển an ninh mạng được quy định như thế nào?

Trả lời:

Nghiên cứu, phát triển an ninh mạng gồm các nội dung sau đây:

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

- 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;

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

- 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;

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

- Giải quyết nguy cơ đe dọa an ninh mạng;

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

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

- Dự báo an ninh mạng;

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

Câu 23. Nhà nước có chính sách như thế nào để nâng cao năng lực tự chủ về an ninh mạng?

Trả lời:

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.

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:

- 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;

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

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

- 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.

Câu 24. Việc tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng được quy định như thế nào?

Trả lời:

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.

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

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 ngoài nước.

Câu 25. Chính sách của Nhà nước và trách nhiệm của các Bộ, ngành, địa phương trong phổ biến kiến thức về an ninh mạng được quy định như thế nào?

Trả lời:

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.

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.

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.

Câu 26. Luật an ninh mạng quy định như thế nào về bảo vệ trẻ em trên không gian mạng?

Trả lời:

Điều 29 Luật an ninh mạng quy định về bảo vệ trẻ em trên không gian mạng như sau:

- 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.

- 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.

- 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 an ninh mạng và pháp luật về trẻ em.

- 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 gia không gian mạng theo quy định của pháp luật về trẻ em.

- 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.

Câu 27. Thời gian gần đây, trên mạng xã hội Facebook liên tiếp đăng những tin đồn thất thiệt, không chính xác như bắt cóc trẻ em ở Cao Bằng, máy bay rơi ở Nội Bài, vỡ đập thủy điện... đã gây hoang mang dư luận và gây thiệt hại đối với tổ chức, cá nhân. Xin hỏi, việc đưa các tin thất thiệt này trên mạng xã hội có vi phạm pháp luật không và sẽ bị xử lý ra sao?

Trả lời:

Các hành vi nêu trên đã vi phạm pháp luật, cụ thể là:

Vi phạm điểm d khoản 1 Điều 8 Luật an ninh mạng, đây là hành vi *"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".*

Vi phạm Điều 5 Nghị định 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, một trong những hành vi bị cấm đó là việc: *Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân….*

Theo Nghị định 174/2013/NĐ-CP ngày 13/11/2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện, với hành vi cung cấp nội dung thông tin sai sự thật, vu khống, xuyên tạc, xúc phạm uy tín của cơ quan, tổ chức và danh dự, nhân phẩm của cá nhân sẽ bị phạt từ 20 triệu đồng đến 30 triệu đồng (điểm a, khoản 3, Điều 64 Nghị định 174/2013/NĐ-CP).

Ngoài ra, việc đưa các tin đồn gây thất thiệt cũng có thể bị xử lý hình sự, tùy vào mức độ vi phạm. Bộ luật hình sự quy định hành vi bịa đặt, loan truyền thông tin sai sự thật nếu có dấu hiệu thỏa mãn yếu tố cấu thành tội phạm có thể bị khởi tố về Tội vu khống (Điều 156 Bộ luật hình sự năm 2015): Người nào bịa đặt hoặc loan truyền những điều biết rõ là sai sự thật nhằm xúc phạm nghiêm trọng nhân phẩm, danh dự hoặc gây thiệt hại đến quyền, lợi ích hợp pháp của người khác hoặc bịa đặt người khác phạm tội và tố cáo họ trước cơ quan có thẩm quyền thì bị phạt từ 10 triệu đồng đến 50 triệu đồng, phạt cải tạo không giam giữ đến 2 năm hoặc phạt tù từ 3 tháng đến 1 năm; trường hợp sử dụng mạng máy tính hoặc mạng viễn thông, phương tiện điện tử để phạm tội thì bị phạt tù từ 01 năm đến 03 năm.

Câu 28. A và H yêu nhau được 02 năm thì chia tay, H có người yêu khác. Biết H có người yêu mới, do hận thù, A đã đăng tải, chia sẻ video ghi lại cảnh nóng giữa A và H trên trang facebook và nhiều lời nói xúc phạm H. Xin hỏi, hành vi của A có vi phạm pháp luật không? hành vi của A sẽ bị xử lý như thế nào?

Trả lời:

Hành vi của A đã vi phạm pháp luật, cụ thể là: Vi phạm quy định tại Điều 5 Nghị định 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng (nghiêm cấm việc lợi dụng dịch vụ Internet và thông tin trên mạng nhằm vào mục đích đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân); Vi phạm quy định tại Điều 8 Luật an ninh mạng (nghiêm cấm việc đăng tải thông tin xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác).

Nếu chưa đủ yếu tố cấu thành tội phạm, hành vi đăng tải, chia sẻ video ghi lại cảnh nóng giữa A và H lên mạng sẽ bị xử lý hành chính. Khoản 3 Điều 66 Nghị định 174/2013 của Chính phủ về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện cũng quy định xử phạt đối với hành vi cung cấp, trao đổi, truyền đưa hoặc lưu trữ, sử dụng thông tin số nhằm đe dọa, quấy rối, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của người khác với số tiền từ 10 triệu đồng đến 20 triệu đồng.

Hành vi của A cũng có thể bị truy cứu trách nhiệm hình sự với tội danh truyền bá văn hoá phẩm đồi trụy, tội làm nhục người khác theo quy định tại Bộ luật hình sự năm 2015.

Câu 29. Anh B là sinh viên năm thứ tư của một trường Đại học công nghệ thông tin, A đã xin được một đoạn mã độc lấy cắp thông tin cá nhân và đã phát tán trên mạng xã hội, A đã thu lợi bất chính 120 triệu đồng từ việc phát tán mã độc. Xin hỏi hành vi cố ý phát tán virut gây hại cho hoạt động của mạng máy tính nhằm thu lợi bất chính sẽ bị xử lý như thế nào theo quy định của Bộ luật hình sự ?

Trả lời:

Theo quy định tại Khoản 1 Điều 286 Bộ luật hình sự năm 2015 quy định tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử như sau:

"*Người nào cố ý phát tán chương trình tin học gây hại cho mạng máy tính, mạng viễn thông, phương tiện điện tử thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 50.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm:*

- Thu lợi bất chính từ 50.000.000 đồng đến dưới 200.000.000 đồng;

- Gây thiệt hại từ 50.000.000 đồng đến dưới 300.000.000 đồng;

- Làm lây nhiễm từ 50 phương tiện điện tử đến dưới 200 phương tiện điện tử hoặc hệ thống thông tin có từ 50 người sử dụng đến dưới 200 người sử dụng;

- Đã bị xử phạt vi phạm hành chính về hành vi này hoặc đã bị kết án về tội này, chưa được xóa án tích mà còn vi phạm".

Đối chiếu với các quy định nêu trên thi hành vi của B sẽ bị xử phạt phạt tiền từ 50.000.000 đồng đến 200.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm. Ngoài ra, B có thể bị cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm (theo Khoản 4 Điều 286 Bộ luật hình sự năm 2015).

Câu 30. Hành vi cá độ bóng đá trên mạng có được coi là hành vi đánh bạc trái phép không? Hành vi này sẽ bị xử lý hình sự như thế nào?

Trả lời:

Trước hết phải khẳng định rằng hành vi cá độ bóng đá, tổ chức cá độ bóng đá là hành vi đánh bạc trái phép.

Nghị quyết số 01/2010/NQ-HĐTP ngày 22/10/2010 của Hội đồng Thẩm phán Tòa án nhân dân tối cao quy định: "Đánh bạc trái phép" là hành vi đánh bạc được thực hiện dưới bất kỳ hình thức nào với mục đích được thua bằng tiền

hay hiện vật mà không được cơ quan nhà nước có thẩm quyền cho phép hoặc được cơ quan nhà nước có thẩm quyền cho phép nhưng thực hiện không đúng với quy định trong giấy phép được cấp.

Điều 321 Bộ luật hình sự năm 2015 quy định về Tội đánh bạc như sau:

" 1. Người nào đánh bạc trái phép dưới bất kỳ hình thức nào được thua bằng tiền hay hiện vật trị giá từ 5.000.000 đồng đến dưới 50.000.000 đồng hoặc dưới 5.000.000 đồng nhưng đã bị xử phạt vi phạm hành chính về hành vi này hoặc hành vi quy định tại Điều 322 của Bộ luật này hoặc đã bị kết án về tội này hoặc tội quy định tại Điều 322 của Bộ luật này, chưa được xóa án tích mà còn vi phạm, thì bị phạt tiền từ 20.000.000 đồng đến 100.000.000 đồng, phạt cải tạo không giam giữ đến 03 năm hoặc phạt tù từ 06 tháng đến 03 năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 03 năm đến 07 năm:

a) Có tính chất chuyên nghiệp;

b) Tiền hoặc hiện vật dùng đánh bạc trị giá 50.000.000 đồng trở lên;

c) Sử dụng mạng internet, mạng máy tính, mạng viễn thông, phương tiện điện tử để phạm tội;

d) Tái phạm nguy hiểm.

3. Người phạm tội còn có thể bị phạt tiền từ 10.000.000 đồng đến 50.000.000 đồng".

Câu 31. Xin hỏi mức xử phạt hành chính đối với hành vi sử dụng mạng nhằm chiếm đoạt tài sản được quy định như thế nào?

Trả lời:

Điều 74 Nghị định 174/2013/NĐ-CP ngày 13/11/2013 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện quy định:

"1. Phạt tiền từ 30.000.000 đồng đến 50.000.000 đồng đối với một trong các hành vi sau đây:

a) Trộm cắp, sử dụng trái phép thông tin về tài khoản, thẻ ngân hàng của tổ chức, cá nhân để chiếm đoạt, gây thiệt hại tài sản;

b) Lừa đảo qua các phương tiện giao tiếp trực tuyến trên mạng Internet, mạng viễn thông nhằm chiếm đoạt tài sản của tổ chức, cá nhân.

2. Phạt tiền từ 50.000.000 đồng đến 70.000.000 đồng đối với một trong các hành vi sau đây:

a) Truy cập bất hợp pháp vào tài khoản của tổ chức, cá nhân nhằm chiếm đoạt tài sản;

b) Thiết lập hệ thống, cung cấp dịch vụ chuyển cuộc gọi quốc tế thành cuộc gọi trong nước phục vụ cho mục đích lừa đảo, chiếm đoạt tài sản.

3.Phạt tiền từ 100.000.000 đồng đến 140.000.000 đồng đối với hành vi lừa đảo trong thương mại điện tử, kinh doanh tiền tệ, huy động vốn tín dụng, mua bán và thanh toán cổ phiếu qua mạng nhằm chiếm đoạt tài sản của tổ chức, cá nhân"

Ngoài việc bị phạt tiền, tổ chức, cá nhân vi phạm còn bị tịch thu tang vật, phương tiện vi phạm; buộc nộp lại số lợi bất hợp pháp có được..

Câu 32: Tôi xin hỏi: người ta nói là đưa thông tin xấu lên mạng sẽ bị xử phạt, tôi thấy những người đưa thông tin lên đã đành, nhưng những người like (thích) hay comment (bình luận) bên dưới với những lời lẽ thiếu văn hoá, hay những quan điểm chủ quan, cá nhân thì cũng cần xử lý đúng không?

Trả lời:

"Lời lẽ thiếu văn hóa", có thể hiểu đó là lời lẽ tục tĩu, khinh miệt, coi thường thậm chí là nhục mạ, vu khống xúc phạm danh dự, nhân phẩm, uy tín người khác.

Tùy vào mức độ của những "lời lẽ thiếu văn hóa" mà chủ thể thực hiện có thể bị xử lý với chế tài tương ứng bằng hành chính hoặc hình sự, cụ thể là:

Nếu những lời bình luận của người đó nhằm mục đích đe dọa, quấy rối, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của người khác thì người thực hiện hành vi này có thể bị phạt tiền từ 10 triệu đồng đến 20 triệu đồng theo quy định tại Điểm g Khoản 3 Điều 66 Nghị định 174/2013/NĐ-CP.

Nếu đủ yếu tố cấu thành tội phạm, hành vi xúc phạm nghiêm trọng danh dự, nhân phẩm người khác thì có thể truy cứu trách nhiệm hình sự về "Tội làm nhục người khác" quy định tại Điều 155 Bộ luật hình sự năm 2015:

"1. Người nào xúc phạm nghiêm trọng nhân phẩm, danh dự của người khác, thì bị phạt cảnh cáo, phạt tiền từ 10.000.000 đồng đến 30.000.000 đồng hoặc phạt cải tạo không giam giữ đến 03 năm.

2. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 03 tháng đến 02 năm:

a) Phạm tội 02 lần trở lên;

b) Đối với 02 người trở lên;

c) Lợi dụng chức vụ, quyền hạn;

d) Đối với người đang thi hành công vụ;

đ) Đối với người dạy dỗ, nuôi dưỡng, chăm sóc, chữa bệnh cho mình;

e) Sử dụng mạng máy tính hoặc mạng viễn thông, phương tiện điện tử để phạm tội;

g) Gây rối loạn tâm thần và hành vi của nạn nhân mà tỷ lệ tổn thương cơ thể từ 31% đến 60%.

3. Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 02 năm đến 05 năm:

a) Gây rối loạn tâm thần và hành vi của nạn nhân mà tỷ lệ tổn thương cơ thể 61% trở lên;

b) Làm nạn nhân tự sát.

4. Người phạm tội còn có thể bị cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm".

Trong trường hợp nếu họ đưa ra những quan điểm chủ quan, cá nhân mà không nhằm mục đích trên thì sẽ không bị xử phạt.

Câu 33. Những người đăng tải thông tin trái văn hoá, đạo đức truyền thống, tuyên truyền kích động bằng những luận điệu chủ quan chống lại Đảng, Nhà nước là xấu độc và bị xử lý. Tôi xin hỏi, nếu chỉ là người chia sẻ đoạn video hay status (trạng thái, tình trạng) nào đó có nội dung xấu nêu trên mà không phải là người đăng tải thì có bị xử lý không?

Trả lời:

Luật an ninh mạng quy định nghiêm cấm các hành vi đăng tải thông tin trái văn hoá, đạo đức truyền thống, tuyên truyền kích động bằng những luận điệu chủ quan chống lại Đảng, Nhà nước và tùy theo mức độ, tính chất mà bị xử lý hành chính hoặc chịu trách nhiệm hình sự.

Những người không đăng tải nhưng có chia sẻ clip hay status có nội dung xấu cũng có thể bị xử lý.

Ví dụ: Khái niệm "phát tán, truyền bá văn hóa phẩm đồi trụy" trước đây vẫn được hiểu nôm na như hành vi mua bán băng đĩa có nội dung tình dục, đăng tải, chia sẻ video, hình ảnh phản cảm, khiêu dâm lên diễn đàn, mạng xã hội. Tuy

nhiên có một động thái đơn giản nhưng cũng được xem là vi phạm pháp luật, đó là khi người dùng dù không đăng tải nhưng đã trực tiếp share (chia sẻ) những thông tin nhạy cảm đó lên trang cá nhân, lên các hội nhóm, hoặc với bạn bè.

Người này có thể sẽ bị truy cứu trách nhiệm hình sự về tội "Truyền bá văn hóa phẩm đồi trụy" hay tội "Làm nhục người khác" theo điều quy định của Bộ luật hình sự năm 2015.

Câu 34. Xin hỏi hành vi vượt qua tường lửa, chiếm tài khoản quản trị Trang thông tin của Sở Nông nghiệp tỉnh A và lấy cắp thông tin, làm sai lệch thông tin, dịch vụ công trên Trang thông tin điện tử Sở Nông nghiệp. Xin hỏi, hành vi nêu trên sẽ bị xử lý như thế nào khi bị truy cứu trách nhiệm hình sự?

Trả lời:

Điều 289 Bộ luật hình sự năm 2015 quy định cụ thể chế tài xử lý đối với hành vi nêu trên, cụ thể như sau:

Người nào cố ý vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của phương tiện điện tử; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ, thì bị phạt tiền từ 50.000.000 đồng đến 300.000.000 đồng hoặc phạt tù từ 01 năm đến 05 năm.

Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 300.000.000 đồng đến 1.000.000.000 đồng hoặc bị phạt tù từ 03 năm đến 07 năm:

- Có tổ chức;

- Lợi dụng chức vụ, quyền hạn;

- Thu lợi bất chính từ 200.000.000 đồng đến dưới 500.000.000 đồng;

- Gây thiệt hại từ 300.000.000 đồng đến dưới 1.000.000.000 đồng;

- Đối với trạm trung chuyển internet quốc gia, hệ thống cơ Sở dữ liệu tên miền và hệ thống máy chủ tên miền quốc gia;

- Tái phạm nguy hiểm.

Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm:

- Đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh;

- Đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông;

- Thu lợi bất chính 500.000.000 đồng trở lên;

- Gây thiệt hại 1.000.000.000 đồng trở lên.

Người phạm tội còn có thể bị phạt tiền từ 5.000.000 đồng đến 50.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.