КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 19 червня 2019 р. N 518

Київ

Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури

Відповідно до частини другої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" Кабінет Міністрів України **постановляє**:

Затвердити Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, що додаються.

Прем'єр-міністр України **В. ГРОЙСМАН**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 19 червня 2019 р. N 518

ЗАГАЛЬНІ ВИМОГИ
до кіберзахисту об'єктів критичної інфраструктури

1. Ці Загальні вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

2. У цих Загальних вимогах терміни вживаються у такому значенні:

критичні бізнес/операційні процеси об'єкта критичної інфраструктури - процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об'єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та /

або становить загрозу для суспільства, життя і здоров'я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-телекомунікаційних систем;

система інформаційної безпеки - сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушенню функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та функціонуванням засобів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

політика інформаційної безпеки - політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-телекомунікаційних системах", Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. N 373 (Офіційний вісник України, 2006 р., N 13, ст. 878).

3. Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

4. Кіберзахист об'єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

5. Кіберзахист об'єкта критичної інфраструктури забезпечується власником та/або керівником об'єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.

6. У випадку, якщо на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

7. У випадку, якщо на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об'єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури.

Створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005.

Власник та/або керівник об'єкта критичної інфраструктури організовує проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки.

8. Власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди

реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

9. Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-телекомунікаційні системи закордонних дипломатичних установ України.

10. Власник та/або керівник об'єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та критичних бізнес/операційних процесів об'єкта критичної інфраструктури для оперативного їх відновлення у разі пошкодження або знищення.

Державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

11. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують ресурси Національної телекомунікаційної мережі.

12. Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні забезпечувати:

формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;

управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

реєстрацію подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;

мережевий захист компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

доступність та відмовостійкість компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, наведено у додатку.

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури може бути доповнено відповідно до технології обробки інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, особливостей функціонування та програмно-апаратного складу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, складу інформаційних ресурсів та компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які підлягають захисту, тощо.

Під час доповнення переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури для кожної загрози об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури передбачаються захід або комплекс заходів, що забезпечують блокування однієї чи декількох загроз або знижують ризик її реалізації, та враховуються умови функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. У разі коли перелік мінімальних заходів не дає можливості забезпечити блокування (нейтралізацію) усіх загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні бути визначені додаткові заходи, які ці загрози блокують.

Формування додаткових заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури розробник комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури здійснює з урахуванням вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

13. У разі відсутності можливості виконання окремих вимог із забезпечення кіберзахисту, наведених у додатку, і/або неможливості їх застосування до окремих об'єктів захисту чи користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, у тому числі внаслідок їх можливого негативного впливу на функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, або неможливості їх здійснення на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури через особливості функціонування, або відсутності складу компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути розроблені і впроваджені компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, або обґрунтовано виключені окремі вимоги з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Власник та/або керівник об'єкта критичної інфраструктури у ході розроблення організаційних і технічних заходів щодо забезпечення кіберзахисту об'єкта критичної інфраструктури обґрунтовує застосування компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури. При цьому під час проведення незалежного аудиту інформаційної безпеки об'єкта критичної інфраструктури або державної експертизи комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури має бути оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та зменшення ризиків об'єкта критичної інфраструктури, або обґрунтованість виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Рішення з обґрунтуванням щодо впровадження компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури оформлюється окремим рішенням за підписом власника та/або керівника об'єкта критичної інфраструктури.

14. Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління. Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв'язку.

СБУ має право подавати міністерствам та іншим центральним органам виконавчої влади обов'язкові для розгляду пропозиції щодо таких вимог з кіберзахисту.

Додаток
до Загальних вимог

ПЕРЕЛІК
базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури

Формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки

1. Об'єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на об'єкті критичної інфраструктури, та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки.

Підрозділ або посадова особа з інформаційної безпеки повинні бути підпорядковані безпосередньо керівнику об'єкта критичної інфраструктури.

Функції підрозділу або посадової особи з інформаційної безпеки можуть бути покладені на службу захисту інформації підприємства, установи, організації.

2. На об'єкті критичної інфраструктури повинні бути визначені права та обов'язки всіх категорій користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, обов'язки адміністраторів з обслуговування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (далі - компоненти об'єкта) та забезпечення її інформаційної безпеки, які оформлюються окремим рішенням за підписом власника та/або керівника об'єкта критичної інфраструктури.

На об'єкті критичної інфраструктури повинні бути призначені відповідальні за функціонування та інформаційну безпеку критичних бізнес/операційних процесів з числа керівників об'єкта критичної інфраструктури, працівники яких забезпечують функціонування цих критичних процесів.

3. На об'єкті критичної інфраструктури повинен бути визначений перелік інформаційних, програмних та апаратних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, рівень їх критичності для об'єкта критичної інфраструктури та/або функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушення функціонування компонентів об'єкта.

4. На об'єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення. Методичною основою для вибору методики є стандарт ДСТУ ISO/IEC 27005.

5. Власник/керівник об'єкта критичної інфраструктури зобов'язаний не рідше одного разу на рік організовувати та проводити обстеження своїх об'єктів критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою оновлення даних щодо програмно-апаратного складу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, технології обробки інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, переліку критичних інформаційних ресурсів та компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які підлягають захисту, тощо. Методичною основою для проведення обстеження об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури є вимоги нормативного документа системи технічного захисту інформації 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі".

Якщо за результатами обстеження об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури виявлено, що на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури змінено технологію обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів об'єкта, які підлягають захисту, тощо, здійснюється перегляд переліку загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, ризиків інформаційної безпеки та рівня прийнятного ризику.

У випадку виявлення нових загроз та/або ризиків здійснюється оновлення технічного завдання на створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, іншої документації та впровадження оновлених вимог на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

6. Власник/керівник об'єкта критичної інфраструктури зобов'язаний забезпечити розроблення та підтримання в актуальному стані технічної, проектної та іншої документації на комплексну систему захисту інформації (систему інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (в захищеній від модифікації формі, зокрема електронній) з обов'язковим описом реалізованих у системі організаційних та технічних заходів безпеки інформації.

Мінімальний перелік документації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури визначається в технічному завданні на створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Програмні та апаратні компоненти об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути налаштовані відповідно до затвердженої політики інформаційної безпеки та технічної, проектної та іншої документації на комплексну систему захисту інформації (систему інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

В інтересах національної безпеки інформація щодо програмно-апаратного складу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, налаштування та конфігураційна інформація програмних та апаратних компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, інформація про параметри та режими їх функціонування, журнали реєстрації подій (логи) та дані аудиту компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, інформація про облікові записи користувачів, їх атрибути та права доступу, об'єкти захисту та їх атрибути доступу, інша

інформація, яка розкриває параметри та особливості функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, є інформацією з обмеженим доступом. Ступінь обмеження доступу до цієї інформації визначається відповідно до закону.

7. На об'єкті критичної інфраструктури необхідно затвердити політику інформаційної безпеки, яка визначає:

мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо на об'єкті критичної інфраструктури;

опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які задіяні в цьому процесі;

вимоги до порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів об'єкта та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами. При цьому необхідно дотримуватися принципу надання необхідних та мінімально достатніх повноважень користувачам та адміністраторам відповідно до їх службових обов'язків;

політику фізичної безпеки та захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури від навколишнього природного середовища;

вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками;

політику управління обліковими записами в програмному та апаратному забезпеченні об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Політика повинна визначати порядок створення, блокування та зупинення облікових записів користувачів та адміністраторів в компонентах об'єкта;

вимоги до порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Повинні бути визначені також вимоги до складності паролів, періодичності їх зміни, блокування роботи користувача за певної кількості спроб підбору пароля, порядок поводження із зовнішніми носіями автентифікаційних даних тощо;

політику забезпечення безперебійної роботи об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, зокрема порядок резервування даних та компонентів об'єкта, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів об'єкта у випадку виходу їх з ладу тощо;

порядок дій персоналу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури у випадках відмов або збоїв об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури в цілому або окремих його компонентів;

порядок використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

політику мережевого захисту, зокрема щодо сегментації мережі об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо;

політику проведення модернізації (оновлення) компонентів об'єкта, внесення змін до складу та в налаштування компонентів об'єкта. Повинні бути визначені відповідальні особи, які мають право проводити ці робити, а також порядок дотримання політики безпеки, яка прийнята на об'єкті критичної інфраструктури, під час проведення таких робіт;

опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які задіяні в цьому процесі;

політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів об'єкта);

політику реєстрації та аудиту подій, що реєструються компонентами об'єкта. Політика повинна містити перелік подій, які реєструються кожним компонентом об'єкта, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на предмет виявлення ознак кібератак або кіберінцидентів;

політику управління інцидентами кібербезпеки, яка повинна містити перелік подій, що кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів у разі їх виникнення, порядок інформування посадових осіб об'єкта критичної інфраструктури, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп'ютерні надзвичайні події);

політику використання електронної пошти користувачами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

політику проведення внутрішнього аудиту інформаційної безпеки об'єкта критичної інфраструктури.

Політика інформаційної безпеки може затверджуватися окремими рішеннями за підписом власника та/або керівника об'єкта критичної інфраструктури. Повинен бути встановлений порядок внесення змін до таких документів.

8. Вимоги затвердженої на об'єкті критичної інфраструктури політики інформаційної безпеки повинні бути доведені під підпис або в інший спосіб до всіх його працівників. На об'єкті критичної інфраструктури повинна бути визначена відповідальність його співробітників за порушення встановленої політики інформаційної безпеки.

9. Власник/керівник об'єкта критичної інфраструктури повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності.

10. У підрозділі або посадової особи з інформаційної безпеки об'єкта критичної інфраструктури повинен бути створений та підтримуватися в актуальному стані перелік програмного та апаратного забезпечення, що використовується на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури в захищеній від модифікації формі, зокрема електронній.

Управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

11. Механізм розподілу прав доступу до об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинен:

охоплювати всі інформаційні ресурси об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (інформацію, яка зберігається та обробляється на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, технологічну інформацію програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, журнали реєстрації подій тощо);

визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (читання, модифікація, створення, видалення тощо);

за необхідності також визначати права доступу користувачів та адміністраторів до служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

12. За можливості реалізації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна надаватися перевага централізованому поширенню інформації щодо налаштувань прав та атрибутів доступу, параметрів реєстрації подій, інших параметрів безпеки та системних налаштувань компонентів об'єкта.

Ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

13. Користувачі та адміністратори об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (за необхідності також активні процеси) повинні отримувати доступ до служб (функцій), інформації та компонентів об'єкта в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо).

14. Засоби об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні надавати можливість ідентифікації кожної операції користувача та адміністратора на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх протоколювання в журналах реєстрації подій.

15. Для надання доступу до служб (функцій) та інформації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна використовуватися багатофакторна автентифікація користувачів та адміністраторів. Допускається використання двофакторної автентифікації тільки в тому програмному забезпеченні компонентів об'єкта, яке не підтримує багатофакторну автентифікацію.

16. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути заблоковані або змінені облікові записи адміністраторів та їх паролів, встановлені за замовчуванням, в усіх

компонентах об'єкта. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

17. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів в усіх компонентах об'єкта. Під час звільнення з посади працівника його обліковий запис повинен бути негайно заблокований або видалений в усіх компонентах об'єкта.

18. Обладнання, яке підключається до системи управління технологічними процесами об'єкта критичної інфраструктури, повинно бути ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), а також повинні бути вжиті заходи, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

Реєстрація подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит

19. Компоненти об'єкта повинні забезпечити реєстрацію, збереження в електронних журналах та захист від модифікації інформації щонайменше про такі події:

доступ та дії з інформацією, яка зберігається та обробляється на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, а також з налаштуваннями програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

реєстрація подій, пов'язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів об'єкта;

вхід/вихід користувачів та адміністраторів в/із компонентів об'єкта;

невдалі спроби входу користувачів та адміністраторів на об'єкт критичної інформаційної інфраструктури об'єкта критичної інфраструктури та перевищення граничної кількості спроб введення пароля;

реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах об'єкта;

зміна пароля користувача в компонентах об'єкта;

реєстрація подій, пов'язаних із зміною конфігураційних налаштувань компонентів об'єкта;

спроби здійснення несанкціонованого доступу до ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

негативні результати перевірок цілісності даних та програмного і апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

всі дії адміністратора з журналами реєстрації подій компонентів об'єкта та налаштування ним параметрів реєстрації.

Повний перелік подій, які реєструються компонентами об'єкта, визначається виходячи із встановленої на об'єкті критичної інфраструктури політики інформаційної безпеки.

20. Журнали реєстрації подій компонентів об'єкта повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнали реєстрації повинні містити інформацію, достатню для встановлення користувача, процесу і мережевого об'єкта, що мали відношення до кожної зареєстрованої події.

21. Має бути забезпечений захист журналів реєстрації подій компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури від несанкціонованого доступу, модифікації або руйнування. Електронні журнали реєстрації подій повинні зберігатися не менше ніж один рік з дати реєстрації останньої події.

22. На об'єкті критичної інфраструктури повинно бути впроваджено систему збору та аналізу журналів реєстрації подій програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Така система повинна мати можливість встановлення фільтрів, які дозволяють робити вибірку і аналіз журналів та подій за різними критеріями та за потреби мати інтерфейси обміну з іншими системами.

Оброблення журналів реєстрації подій не повинно впливати на функціонування критичних бізнес/операційних процесів об'єкта критичної інфраструктури.

23. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна бути забезпечена можливість роботи з архівними журналами реєстрації подій за попередні періоди шляхом завантаження журналів на об'єкт критичної інформаційної інфраструктури об'єкта критичної інфраструктури із зовнішнього джерела. При цьому дані, що завантажуються, повинні тільки доповнювати існуючі журнали, але не затирати і не змінювати інформації, що вже зберігається в них.

Архівні журнали реєстрації подій зберігаються на фізично відокремленому компоненті об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури або окремому носії даних не менше року з дати їх утворення.

Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

24. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. Повинно бути забезпечене централізоване управління засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

25. Доступ адміністраторам до компонентів об'єкта повинен надаватися виключно з IP-адрес (робочих станцій), які визначені для адміністрування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

26. У разі неможливості фізичного розділення зовнішньої мережі та об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на межі (периметрі) між зовнішніми мережами, іншими інформаційно-телекомунікаційними системами, що обслуговують об'єкт критичної інфраструктури, та об'єктом критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути встановлені засоби мережевого захисту, що виконують щонайменше такі функції захисту:

захист від атак "нульового дня" (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

фільтрація трафіку та розмежування доступу між мережею об'єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. Блокування трафіку та з'єднань, які не відповідають визначеним критеріям;

фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

захист від атак типу "відмова в обслуговуванні";

захист від несанкціонованого доступу через Інтернет;

балансування навантаження;

маскування структури і мережевих адрес мережі;

завершення з'єднання з вузлом у разі атаки;

здійснення реєстрації подій, що мають відношення до безпеки.

Для захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення.

27. На об'єкті критичної інфраструктури необхідно здійснити розподіл об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.

28. Реалізована архітектура об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна надавати можливість розподілу мережі щонайменше на такі частини / зони:

зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

зона прикладних застосувань об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

зона сховищ даних об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone);

зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;

тестова зона (Test-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, перед тим як впровадити їх в промислову експлуатацію на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

29. Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів / користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури із зовнішніх мереж, повинні бути розміщені в зовнішній зоні об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. З'єднання серверів та обладнання, які розміщені в зовнішній зоні, із серверами та обладнанням внутрішньої мережі об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні захищатися міжмережевим екраном.

30. Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, а також серверні частини засобів захисту інформації повинні бути розміщені в зоні прикладних застосувань системи безпеки (Security-zone) мережі, захищеної за допомогою міжмережевого екрана.

31. Сегмент інформаційної інфраструктури об'єкта критичної інфраструктури, в якому перебуває система керування технологічними процесами, повинен бути відокремленим від інших систем об'єкта критичної інфраструктури. У випадку логічного відокремлення на межі сегмента повинен бути встановлений міжмережевий екран.

32. Повинні бути визначені та відключені (заблоковані) програмні порти компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які є небезпечними для забезпечення кібербезпеки.

33. Власник/керівник об'єкта критичної інфраструктури зобов'язаний проводити перевірку ефективності заходів щодо захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test). У разі отримання негативних результатів після проведення тестів необхідно вжити заходів для усунення їх причин.

34. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури передача даних бездротовими мережами повинна здійснюватися виключно захищеними з'єднаннями із забезпеченням її конфіденційності та цілісності. Забороняється використання на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури технологій Wi-Fi та Bluetooth.

35. Для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та об'єктом критичної інформаційної інфраструктури об'єкта критичної інфраструктури, між компонентами об'єкта (поза контрольованою територією об'єкта критичної інфраструктури), між об'єктом критичної інформаційної інфраструктури об'єкта критичної інфраструктури та іншими (зовнішніми) інформаційно-телекомунікаційними системами, необхідно використовувати захищені з'єднання із забезпеченням конфіденційності та цілісності цих даних.

36. Систему управління технологічними процесами об'єкта інфраструктури дозволяється підключати до глобальних мереж передачі даних, зокрема до Інтернету, тільки у випадку неможливості функціонування технологічного процесу без підключення до Інтернету та за умови впровадження всіх заходів захисту відповідно до Загальних вимог до кіберзахисту об'єктів критичної інфраструктури або конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єкта критичної інфраструктури, який відноситься до відповідної сфери управління.

37. До глобальних мереж передачі даних, зокрема Інтернету, об'єкти критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні підключатися через тих операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю. У договорі з надавачем цих послуг зазначаються зобов'язання щодо виконання тієї частини Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, які він надає об'єкту критичної інформаційної інфраструктури об'єкта критичної інфраструктури, та наявність комплексної системи захисту інформації з підтвердженою відповідністю.

Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

38. Інформаційна інфраструктура об'єкта критичної інфраструктури повинна будуватися на базі відмовостійкого підходу. Для забезпечення відмовостійкості об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинно здійснюватися, як мінімум, таке:

періодичне створення резервних копій інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та критичних бізнес/операційних процесів об'єкта критичної інфраструктури, включаючи інформацію, яка зберігається на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, технологічну інформацію компонентів об'єкта та образів серверів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, а також їх відновлення у випадку втрати або пошкодження;

резервування критичних для функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та бізнес/операційних процесів об'єкта критичної інфраструктури програмних та апаратних компонентів для забезпечення його сталого функціонування у випадку виходу з ладу одного з критичних компонентів. У разі використання на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури віртуальних серверів необхідно забезпечити їх резервування;

дублювання (кластеризація) критичних для функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та бізнес/операційних процесів об'єкта критичної інфраструктури програмних та апаратних компонентів об'єкта для забезпечення його сталого функціонування, зниження навантаження та збільшення продуктивності;

використання засобів балансування навантаження;

використання джерел безперебійного живлення для критичних компонентів об'єкта;

зв'язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами), - для об'єкта критичної інфраструктури, які надають свої послуги через Інтернет.

39. Під час розроблення, модернізації або оновлення компонентів системи управління технологічними процесами об'єкта критичної інфраструктури необхідно використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента його мережі для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення, перед тим як впровадити їх в промислову експлуатацію.

Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури

40. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна проводитися перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

41. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна здійснюватися ідентифікація всіх змінних (зовнішніх) пристроїв та носіїв інформації за допомогою унікального ідентифікатора.

Повинно бути унеможливлено використання змінних (зовнішніх) пристроїв та носіїв інформації, які не зареєстровані на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

42. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинно бути відключено автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації.

43. Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

44. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна проводитися перевірка на цілісність та автентичність оновлень компонентів об'єкта. У разі порушення цілісності або непідтвердження автентичності оновлення воно повинно бути відхилене і не повинно застосовуватися, а цю подію необхідно запротоколювати в журналі подій.

45. У складі об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинно використовуватися програмне та апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватися офіційні стабільні версії прикладного програмного забезпечення та драйверів.

На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна надаватися перевага програмному забезпеченню, яке має більш вищий рівень гарантій відповідно до нормативного документа системи технічного захисту інформації 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", за результатами державної експертизи у сфері технічного захисту інформації.

46. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинно блокуватися самостійне встановлення або видалення користувачами програмного забезпечення на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор.

47. Засоби об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні забезпечувати неприйняття файла/повідомлення в обробку у разі отримання негативного результату перевірки електронного підпису файла/повідомлення, що надійшов/надійшло. Ця подія повинна відображатися в журналі реєстрації подій.

48. Програмні та апаратні засоби, які використовуються у складі об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, не повинні мати походження з іноземної держави, до якої застосовано санкції згідно із Законом України "Про санкції", чи бути розроблені/виготовлені юридичною особою - резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

Визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

49. Компоненти та/або інформація об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, крім систем управління технологічними процесами, можуть перебувати в сторонньому (не власному) центрі обробки даних тільки за умови, що центр обробки даних розташований на території України (за винятком тимчасово окупованої території України), а власником центру обробки даних є резидент України. При цьому у договорі із центром обробки даних повинні зазначатися його зобов'язання щодо виконання тієї частини Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, які він надає об'єкту критичної інфраструктури.

Компоненти та інформація (дані) систем управління технологічними процесами об'єкта критичної інфраструктури повинні бути розміщені тільки у власному центрі обробки даних.

50. З метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення державні органи використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

51. Компоненти об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні розміщуватися у приміщеннях, які унеможливлюють несанкціонований фізичний доступ до них сторонніх осіб.

Повинен бути забезпечений контрольований фізичний доступ до приміщень та/або комутаційних шаф, де розташовані робочі станції, сервери, мережеві компоненти та комутаційні вузли структурованої кабельної системи об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

52. Забороняється підключати робочі місця адміністраторів та операторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури до інших інформаційно-телекомунікаційних систем.

53. Схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, схеми підключення обладнання,

таблиці маркування кабелів структурованої кабельної системи та кабельних з'єднань зберігаються в актуальному стані.
