Опис вимог базового профілю безпеки інформації

(наказ Адміністрації Держспецзв'язку від 24.06.2024 № 317 «Про визначення Базового профілю безпеки інформації»)

№	Назва вимоги	Опис вимоги
1.	**Управління доступом**	
1.1.	Управління обліковими записами	Ця вимога зосереджена на управлінні обліковими записами для систем і додатків. Визначення та застосування дозволів на доступ, відмінних від тих, що визначаються типом облікового запису (наприклад, привілейований доступ, непривілейований доступ), розглядаються у вимозі 1.2. Типи облікових записів в системі включають індивідуальні, групові, тимчасові, системні, гостьові, анонімні, аварійні, розробника та сервісні. Користувачі, яким потрібні адміністративні привілеї облікових записах в системі, проходять додаткову перевірку персоналом організації, відповідальним за затвердження таких облікових записів і привілейованого доступу. Типи облікових записів, які організації можуть заборонити через підвищений ризик, включають групові, аварійні, гостьові, анонімні та тимчасові. Організації можуть визначати привілеї доступу або інші атрибути за обліковими записами, типами облікових записів або їх комбінацією. Інші атрибути, необхідні для авторизації доступу, включають обмеження на час доби, день тижня та джерело походження. Визначаючи інші атрибути облікових записів, організації враховують вимоги системи (наприклад, оновлення системи, планове обслуговування), а також вимоги місії та бізнесу (наприклад, різниця в часових поясах, віддалений доступ під час відряджень). До користувачів, які становлять значний ризик для безпеки, належать особи, щодо яких є достовірні докази того, що вони мають намір використати санкціонований доступ до системи для завдання шкоди, або що зловмисники намагатимуться завдати шкоди через них. Тісна координація між менеджерами з управління персоналом, власниками місії/бізнесу, адміністраторами системи та юридичним персоналом є дуже важливою при відключенні облікових записів системи осіб, які становлять значний ризик. Періоди часу для повідомлення персоналу організації можуть бути різними.
1.2.	Забезпечення доступу	Політики управління доступом контролюють доступ між активними об'єктами або суб'єктами (тобто користувачами або процесами в системі, що діють від імені користувачів) і пасивними об'єктами або суб'єктами (тобто пристроями, файлами, записами, доменами) в системах організації. Типи доступу до системи включають віддалений доступ і доступ до систем, що взаємодіють через зовнішні мережі, такі як Інтернет. Механізми розмежування доступу також можуть

№	Назва вимоги	Опис вимоги
		бути застосовані на рівні додатків і сервісів, щоб забезпечити підвищений захист інтерфейсу користувача. При цьому визнається, що система може містити багато додатків і сервісів для підтримки діяльності та бізнес-функцій.
1.3.	Управління інформаційними потоками	Управління інформаційними потоками регулює, куди може переміщатися інформація в межах системи та між системами (і хто може отримати доступ до інформації), без явного врахування подальших доступів до цієї інформації. Управління обмеженнями потоками включають наступне: запобігання відкритій передачі інформації в інтернет, блокування зовнішнього трафіку, який видає себе за внутрішній, обмеження запитів до інтернету, які не надходять від внутрішнього веб-проксі-сервера, а також обмеження передачі інформації між організаціями на основі структур даних і контенту. Організації зазвичай використовують політики та механізми контролю потоків інформації для управління потоками інформації між визначеними джерелами та одержувачами (наприклад, мережами, особами та пристроями) всередині систем та між взаємопов'язаними системами. Управління потоком базується на характеристиках інформації або структурі інформаційних потоків. Забезпечення виконання відбувається в пристроях захисту на кордоні системи(наприклад, зашифрованих тунелях, маршрутизаторах, шлюзах і брандмауерах), які використовують набори правил або встановлюють параметри конфігурації, що обмежують сервіси в системі, забезпечують фільтрацію пакетів на основі заголовків або фільтрацію повідомлень на основі їхнього змісту (наприклад, здійснюючи пошук за ключовими словами або використовуючи характеристики документів). Організації також враховують надійність механізмів фільтрації та перевірки (тобто апаратних засобів, прошивки та програмних компонентів), які є критично важливими для забезпечення захисту інформаційних потоків. Передача інформації між системами, які представляють різні домени безпеки з різними політиками безпеки, створює ризик того, що така передача порушує одну або кілька політик безпеки домену. У таких ситуаціях власники інформації або адміністратори надають вказівки у визначених точках застосування політик між взаємопов'язаними системами. Організації розглядають можливість запровадження певних архітектурних рішень, коли це необхідно для забезпечення дотримання певних політик безпеки. Забезпечення виконання включає заборону передачі інформації між взаємопов'язаними системами (тобто, дозвіл лише на доступ до інформації), використання апаратних механізмів для забезпечення односторонніх інформаційних потоків, а також

№	Назва вимоги	Опис вимоги
		впровадження надійних механізмів перепризначення атрибутів безпеки та міток безпеки.
1.4.	Розмежування обов’язків	Розмежування обов'язків усуває потенційну можливість зловживання наданими привілеями та знижує ризик зловмисної діяльності без змови. Розмежування обов'язків передбачає розподіл функцій завдань і функцій підтримки між різними особами або ролями, виконання функцій підтримки системи різними особами або ролями (наприклад, забезпечення якості, управління конфігурацією, управління системою, оцінювання, програмування та мережева безпека), а також забезпечення того, щоб персонал, який адмініструє функції контролю доступу, не виконував також функції аудиту. Оскільки порушення розмежування обов'язків можуть охоплювати системи та домени додатків, організації повинні враховувати всю сукупність своїх систем та компонентів системи при розробці політик розподілу обов'язків. Ця вимога є обов'язковою до виконання з 1.2.
1.5.	Мінімізація повноважень	Організації використовують принцип мінімізації повноважень для виконання певних обов'язків і санкціонованого доступу для користувачів і процесів в системі. Принцип мінімізація повноважень застосовується до розробки, впровадження та експлуатації системи. Організації розглядають можливість створення додаткових процесів, ролей і облікових записів в системі для досягнення мінімізації повноважень. Функції безпеки включають створення облікових записів в системі і призначення привілеїв, встановлення програмного забезпечення, налаштування авторизації доступу, налаштування параметрів для подій, що підлягають аудиту, встановлення параметрів сканування вразливостей і встановлення параметрів виявлення вторгнень. Інформація, що стосується безпеки, включає інформацію про загрози та вразливості, правила фільтрації для маршрутизаторів або брандмауерів, параметри конфігурації служб безпеки, архітектуру безпеки, інформацію про управління криптографічними ключами та списки контролю доступу.
1.6.	Мінімізація повноважень – непривілейований доступ до незахищених функцій	Привілейовані облікові записи зазвичай називають обліковими записами адміністраторів системи. Обмеження привілейованих облікових записів певним персоналом або ролями запобігає доступу непривілейованих користувачів до функцій безпеки або інформації, пов'язаної з безпекою. Вимога використання непривілейованих облікових записів для доступу до функцій, що не стосуються безпеки, або інформації, що не стосується безпеки, обмежує вразливість під час роботи з привілейованими обліковими записами. Включення ролей стосується ситуацій, коли організації впроваджують політики контролю доступу, такі як контроль доступу на основі ролей, і коли зміна ролі забезпечує такий самий ступінь впевненості в зміні

№	Назва вимоги	Опис вимоги
		повноважень доступу для користувача і процесів, що діють від імені користувача, як і зміна між привілейованим і непривілейованим обліковими записами.
1.7.	Мінімізація повноважень – заборона непривілейованим користувачам виконувати привілейовані функції	Привілейовані функції включають створення облікових записів в системі, перевірку цілісності системи, встановлення оновлень або адміністрування криптографічних ключів. Непривілейовані користувачі не мають відповідних повноважень для виконання привілейованих функцій. Обхід механізмів виявлення та запобігання вторгненням або механізмів захисту від шкідливого коду є прикладами привілейованих функцій, які потребують захисту від непривілейованих користувачів. Ця вимога є умовою, яка має бути досягнута шляхом визначення дозволених привілеїв у 1.1. та застосування цих привілеїв у 1.2. Зловживання привілейованими функціями - навмисне чи ненавмисне з боку авторизованих користувачів або неавторизованих зовнішніх суб'єктів, які скомпрометували облікові записи в системі - є серйозною і постійною проблемою, яка може мати значні негативні наслідки для організацій. Реєстрація використання привілейованих функцій - це один із способів виявити такі зловживання та зменшити ризики, пов'язані з внутрішніми та зовнішніми загрозами.
1.8.	Невдалі спроби входу в систему	Через потенційну можливість відмови в обслуговуванні автоматичне блокування системи в більшості випадків є тимчасовим і автоматично розблоковується через заздалегідь визначений період, встановлений організацією (тобто з використанням алгоритму затримки). Організації можуть використовувати різні алгоритми затримки для різних компонентів системи, виходячи з можливостей відповідних компонентів. Реакція на невдалі спроби входу до системи може бути реалізована на рівні системи та програмного забезпечення.
1.9.	Попередження про використання системи	Відображення повідомлень може бути реалізовано за допомогою попереджувальних або банерних повідомлень. Повідомлення відображаються до того, як користувачі увійдуть до системи. Повідомлення про використання системи використовуються лише для доступу через інтерфейси входу за участю користувачів і не є обов'язковими, якщо інтерфейсів не існує. Організації вирішують, чи потрібне вторинне повідомлення про використання для доступу до програм або інших ресурсів в системі після першого входу в мережу. Постери або інші друковані матеріали можуть бути використані замість автоматизованого повідомлення. в системі. Ця вимога стосується 15.3.
1.10.	Блокування пристрою	Блокування пристроїв - це тимчасові дії, що вживаються для запобігання доступу до системи, коли користувачі виходять з безпосередньої близькості до системи, але не

№	Назва вимоги	Опис вимоги
		хочуть виходити з системи через тимчасовий характер своєї відсутності. Блокування пристроїв може бути реалізовано на рівні операційної системи або на рівні програми. Ініційоване користувачем блокування пристрою базується на поведінці або політиці і вимагає від користувача фізичних дій, щоб ініціювати блокування пристрою. Блокування пристроїв не є прийнятною заміною виходу з системи, наприклад, коли організації вимагають від користувачів виходити з системи в кінці робочого дня. Приховані екрани можуть включати статичні або динамічні зображення, такі як візерунки, що використовуються в заставках, фотографічні зображення, суцільні кольори, годинник, індикатор заряду батареї або порожній екран із застереженням про те, що інформація не відображатиметься на екрані.
1.11.	Припинення сеансу	Ця вимога стосується завершення ініційованих користувачем логічних сеансів, на відміну від завершення мережевих з'єднань, які асоціюються з сеансами зв'язку (тобто відключення від мережі) в 13.5. Логічний сеанс ініціюється щоразу, коли користувач (або процеси, що діють від імені користувача) отримує доступ до системи. Логічні сеанси можна завершити (і таким чином завершити доступ користувача) без завершення мережевих сеансів. Завершення сеансу завершує всі процеси в системі, пов'язані з логічним сеансом користувача, за винятком тих процесів, які були створені користувачем (тобто власником сеансу) для продовження роботи після завершення сеансу. Умови або події, які вимагають автоматичного завершення сеансу, можуть включати визначені організацією періоди неактивності користувача, обмеження на використання системи в певний час доби, а також цілеспрямоване реагування на певні типи інцидентів.
1.12.	Віддалений доступ	Віддалений доступ до системи являє собою значну потенційну вразливість, якою можуть скористатися зловмисники. Моніторинг і контроль методів віддаленого доступу дозволяє організаціям виявляти атаки і забезпечувати дотримання політик віддаленого доступу. Це відбувається шляхом аудиту активності з'єднань віддалених користувачів з системами. Маршрутизація віддаленого доступу через керовані точки контролю доступу посилює явний контроль над такими з'єднаннями і знижує вразливість до несанкціонованого доступу до системи, який може призвести до несанкціонованого розкриття інформації. Обмеження виконання привілейованих команд та доступу до інформації, важливої для безпеки, через віддалений доступ зменшує вразливість організації та її сприйнятливість до загроз з боку зловмисників. Привілейована команда - це ініційована людиною команда, що виконується в системі, яка передбачає контроль,

№	Назва вимоги	Опис вимоги
		моніторинг або адміністрування системи, включно з функціями безпеки та інформацією, важливою для безпеки. Інформація, важлива для безпеки - це інформація, яка потенційно може вплинути на роботу функцій безпеки або надання послуг безпеки таким чином, що це може призвести до порушення політики безпеки системи, у тому числі ізоляції програмного коду та даних. Привілейовані команди надають окремим особам можливість виконувати конфіденційні, критичні для безпеки або пов'язані з безпекою функції в системі. Контроль доступу з віддалених місць допомагає гарантувати, що неавторизовані особи не зможуть виконати такі команди, які можуть завдати серйозної або катастрофічної шкоди системі.
1.13.	Бездротовий доступ	Встановлення обмежень використання та вимог до конфігурації/підключення для бездротового доступу до системи надає організаціям критерії для підтримки рішень щодо авторизації бездротового доступу. Такі обмеження та вимоги зменшують вразливість до несанкціонованого доступу до системи за допомогою бездротових технологій. Бездротові мережі використовують протоколи автентифікації, які забезпечують захист облікових даних та взаємну автентифікацію. Організації здійснюють автентифікацію осіб та пристроїв, щоб допомогти захистити бездротовий доступ до системи. Особлива увага приділяється різноманітності пристроїв з потенційним бездротовим доступом до системи, включаючи мобільні пристрої малого форм-фактору (наприклад, смартфони, смарт-годинники). Можливості бездротових мереж, вбудовані в компоненти системи, становлять значну потенційну вразливість, якою можуть скористатися зловмисники. Вимкнення бездротових можливостей, якщо вони не потрібні для виконання важливих завдань або бізнес-функцій, може допомогти зменшити вразливість до загроз з боку зловмисників, пов'язаних з бездротовими технологіями.
1.14.	Контроль доступу для мобільних пристроїв	Мобільний пристрій — це обчислювальний пристрій малого форм-фактора такий, що може легко переноситься однією особою; призначений для роботи без фізичного підключення; має локальний, незнімний або знімний накопичувач даних; і включає автономне джерело живлення. Функціональність мобільних пристроїв може також включати можливості голосового зв'язку, вбудовані датчики, які дозволяють пристрою збирати інформацію, та/або вбудовані функції для синхронізації локальних даних з віддаленими пристроями. Прикладами є смартфони, смарт годинники та планшети. Зазвичай мобільні пристрої пов’язані з однією особою. Можливості обробки, зберігання та передачі даних на мобільних пристроях можуть бути порівнянними з можливостями ноутбуків або настільних комп'ютерів, залежно від характеру та

№	Назва вимоги	Опис вимоги
		призначення пристрою. Захист і контроль мобільних пристроїв базується на поведінці або політиці та вимагає від користувачів фізичних дій, щоб захистити та контролювати такі пристрої, коли вони знаходяться поза контрольованими зонами. Контрольовані зони - це території, для яких організація забезпечує фізичний або процедурний контроль, щоб відповідати вимогам, встановленим для захисту інформації. Через велику різноманітність мобільних пристроїв з різними характеристиками та можливостями, обмеження в організації можуть відрізнятися для різних класів або типів таких пристроїв. Обмеження щодо використання, вимоги до конфігурації та підключення мобільних пристроїв включають управління конфігурацією, ідентифікацію та автентифікацію пристрою, впровадження обов'язкового захисного програмного забезпечення, сканування пристроїв на наявність шкідливого коду, оновлення програмного забезпечення для захисту від вірусів, сканування критично важливих оновлень та виправлень, проведення первинних перевірок цілісності операційної системи (і, можливо, іншого резидентного програмного забезпечення), а також відключення непотрібного апаратного обладнання. Організації можуть використовувати шифрування всього носія інформації пристрою або шифрування на основі контейнерів для захисту конфіденційності інформації на мобільних пристроях. Шифрування на основі контейнерів забезпечує більш тонкий підхід до шифрування даних та інформації, включаючи шифрування вибраних структур даних (наприклад, файлів, записів або полів).
1.15.	Використання зовнішніх систем	Зовнішні системи - це системи, які використовуються організацією, але не є її частиною. До зовнішніх систем відносяться системи, компоненти або пристрої, що знаходяться у приватній власності, а також приватні обчислювальні та комунікаційні пристрої, що знаходяться на комерційних або державних об'єктах; системи, що перебувають у власності або під контролем недержавних організацій; а також системи, що перебувають під управлінням підрядників. Організації мають можливість заборонити використання будь-якого типу зовнішніх систем або певних типів зовнішніх систем (наприклад, заборонити використання зовнішніх систем, які не є власністю організації). Положення та умови узгоджуються з довірчими відносинами, встановленими з організаціями, які володіють, керують або обслуговують зовнішні системи, і включають опис спільної відповідальності. Авторизовані особи - це персонал організації, підрядники або інші особи, які мають авторизований доступ до системи організації та мають повноваження встановлювати конкретні правила щодо доступу до системи. Обмеження, які організації накладають на авторизованих осіб, не

№	Назва вимоги	Опис вимоги
		обов'язково мають бути однаковими, оскільки вони можуть відрізнятися залежно від довірчих відносин між організаціями. Організаціям потрібна впевненість, що зовнішні системи відповідають необхідним вимогам безпеки, щоб не скомпрометувати, не пошкодити або не завдати шкоди системі. Ця вимога є обов'язковою до виконання з 16.3.
1.16.	Публічно доступний контент	Відповідно до чинного законодавства, виконавчих наказів, директив, політик, положень, стандартів і керівних документів, громадськість не має права мати доступ до інформації з обмеженим доступом.
2.	**Обізнаність і навчання**	
2.1.	Навчання з підвищення обізнаності	Організації забезпечують базовий та просунутий рівні навчання обізнаності з питань безпеки для користувачів систем (включаючи менеджерів, вищий виконавчий персонал, адміністраторів системи та підрядників), а також заходи для перевірки рівня знань користувачів. Організації визначають зміст навчання на основі конкретних вимог, систем, до яких персонал має санкціонований доступ, та робочих середовищ (наприклад, дистанційна робота). Зміст включає розуміння необхідності забезпечення безпеки та дій, необхідних від користувачів для підтримання безпеки та реагування на інциденти. Також розглядаються питання безпеки операцій та поводження з інформацією з обмеженим доступом. Методи підвищення обізнаності з питань безпеки включають розміщення плакатів, пропонування матеріалів з нагадуваннями про безпеку, відображення повідомлень на екрані входу в систему, створення електронних повідомлень або повідомлень від посадових осіб організації, а також проведення інформаційних заходів з використанням подкастів, відео та вебінарів. Навчання з безпеки проводиться з періодичністю, що відповідає чинним законам, директивам, правилам і політикам. Регулярне оновлення змісту навчання гарантує, що він залишається актуальним. Подіями, які можуть прискорити оновлення змісту тренінгу, є результати оцінювання або аудиту, інциденти або порушення безпеки, а також зміни в чинному законодавстві, виконавчих наказах, директивах, положеннях, політиках, стандартах і настановах. Потенційними індикаторами та можливими передвісниками внутрішніх загроз є поведінка, наприклад: надмірне, тривале незадоволення роботою; спроби отримати доступ до інформації, яка не потрібна для виконання роботи; необґрунтований доступ до фінансових ресурсів; знущання або сексуальні домагання до колег; насильство на робочому місці; інші серйозні порушення політики, процедур, правил, директив чи практик організації. Організації можуть розглянути можливість

№	Назва вимоги	Опис вимоги
		адаптувати теми підвищення обізнаності про внутрішні загрози до ролі (наприклад, тренінги для керівників можуть бути зосереджені на конкретних змінах у поведінці членів команди, тоді як тренінги для працівників можуть бути зосереджені на більш загальних спостереженнях). Соціальна інженерія - це спроба обманом змусити людину розкрити інформацію або вжити заходів, які можуть бути використані для порушення, компрометації або іншого негативного впливу на систему. Соціальна інженерія включає в себе фішинг, підставу, видавання себе за іншу особу, приманку, послугу за послугу, перехоплення потоку, експлуатацію соціальних мереж, а також "Tailgating". Соціальний майнінг - це спроба зібрати інформацію про організацію, яка може бути використана для підтримки майбутніх атак. Навчання безпековій обізнаності включає в себе інформування працівників та керівництва про потенційні ознаки внутрішньої загрози, а також про потенційні та фактичні випадки соціальної інженерії та видобутку даних через відповідні канали організації згідно з встановленими політиками та процедурами.
2.2.	Рольове навчання	Організації визначають зміст та періодичність навчання з питань безпеки на основі покладених обов'язків, ролей та відповідальності окремих осіб, а також вимог безпеки систем, до яких персонал має авторизований доступ. Крім того, організації забезпечують розробників систем, архітекторів безпеки, розробників програмного забезпечення, інтеграторів системи, посадових осіб, відповідальних за придбання/закупівлі, адміністраторів системи та мережі, персонал, який здійснює управління конфігурацією та аудит, персонал, який виконує незалежну перевірку та валідацію системи безпеки, експертів з оцінки безпеки та персонал, який має доступ до програмного забезпечення в системі, технічною підготовкою з питань безпеки, спеціально розробленою для виконання їхніх обов'язків. Комплексне тренування на основі покладених обов'язків стосується управлінських, операційних і технічних ролей та обов'язків, які охоплюють фізичний, кадровий і технічний контроль. Таке навчання може включати політики, процедури, інструменти та артефакти для визначених ролей у сфері безпеки. Організації також забезпечують навчання, необхідне для виконання окремими особами своїх обов'язків, пов'язаних з операціями постачання та безпекою ланцюгів постачання в контексті програм інформаційної безпеки організації.
3.	**Аудит і підзвітність**	

№	Назва вимоги	Опис вимоги
3.1.	Події аудиту	Подія – це будь-яке спостережуване явище в системі, яке включає спроби виконати несанкціоновану діяльність в системі. Організації визначають типи подій, для яких необхідна функція реєстрації. До них належать події, які мають відношення до безпеки систем і середовищ, в яких ці системи функціонують, для досягнення конкретних і поточних потреб аудиту. Типи подій можуть включати зміну пароля, невдалий вхід в систему або невдалий доступ до систем, використання адміністративних привілеїв. При визначенні типів подій, які вимагають реєстрації, організації розглядають моніторинг та аудит системи, відповідні для кожної з вимог безпеки. Визначаючи типи подій, організації враховують реєстрацію, яка необхідна для охоплення пов'язаних подій, таких як етапи в розподілених процесах на основі транзакцій (наприклад, процеси, розподілені між кількома організаціями) і дії, які відбуваються в сервісно-орієнтованих або хмарних архітектурах. Вимоги до моніторингу та аудиту можуть бути збалансовані з іншими потребами системи. Наприклад, організації можуть визначити, що системи повинні мати можливість реєструвати кожне звернення до файлу, як успішне, так і неуспішне, але не активувати цю можливість за винятком певних обставин через потенційне навантаження на продуктивність системи. Типи подій, які реєструються організаціями, можуть змінюватися з часом. Періодичний перегляд та оновлення набору типів подій, що реєструються, необхідний для того, щоб переконатися, що поточний набір залишається необхідним та достатнім.
3.2.	Зміст записів аудиту	Зміст записів аудиту, який може бути необхідним для підтримки функції аудиту, включає позначки часу, адреси джерела та призначення, ідентифікатори користувачів або процесів, описи подій, індикатори успіху або невдачі, імена файлів, а також правила контролю доступу або управління потоками, що застосовуються. Результати подій можуть включати індикатори успіху або невдачі події та результати, характерні для конкретної події (наприклад, стан безпеки системи після того, як подія відбулася). Детальна інформація, яку організації можуть розглядати в записах аудиту, включає повнотекстові записи привілейованих команд або індивідуальні ідентифікаційні дані користувачів групових облікових записів.
3.3.	Збереження записів аудиту	Записи аудиту можуть генеруватися на різних рівнях архітектури системи, в тому числі на рівні пакетів, коли інформація проходить через мережу. Вибір відповідного рівня архітектури системи є критично важливим аспектом можливості реєстрації записів аудиту і може сприяти виявленню першопричин виникнення проблем. Можливість додавання інформації, згенерованої в записах аудиту, залежить від функціональних можливостей системи для конфігурації вмісту записів аудиту. Організації

№	Назва вимоги	Опис вимоги
		розглядають додаткову інформацію в записах аудиту, включаючи правила контролю доступу або контролю потоків, що застосовуються, та індивідуальні ідентифікаційні дані користувачів групових облікових записів. Організації розглядають можливість обмеження додаткової інформації в журналах аудиту лише тією інформацією, яка явно необхідна для конкретних вимог аудиту.
3.4.	Реагування на відмови обробки даних аудиту	До відмов у процесі обробки даних аудиту належать помилки програмного та апаратного забезпечення, відмови в механізмах реєстрації звітів аудиту, а також досягнення або перевищення ємності сховища даних звітів аудиту. Заходи реагування включають перезапис найстаріших звітів аудиту, вимкнення системи та зупинку реєстрації записів аудиту. Організації можуть визначати додаткові дії для реєстрації збоїв у процесі обробки даних аудиту на основі: типу збою, місцезнаходження збою, серйозності збою, або комбінації таких факторів. Ця вимога застосовується до кожного сховища даних звітів аудиту (тобто окремого компонента системи, де зберігаються звіти аудиту), загальної ємності сховища даних звітів аудиту організацій (тобто всіх сховищ даних звітів аудиту разом узятих) або до обох. Організації можуть вирішити не вживати жодних додаткових заходів після попередження визначених ролей або персоналу.
3.5.	Огляд, аналіз і звітність аудиту	Перегляд, аналіз та звітування записів аудиту охоплюють ведення журналів інформаційної безпеки в організаціях і можуть включати записи, отримані в результаті моніторингу використання облікових записів, віддаленого доступу, бездротового з'єднання, налаштувань конфігурації, використання інструментів технічного обслуговування та віддаленого обслуговування, інвентаризації компонентів системи, підключення мобільних пристроїв, встановлення та вилучення обладнання, фізичного доступу, температури та вологості, комунікації на інтерфейсах системи та використання мобільного коду. Про результати можна повідомляти таким підрозділам організації, як група реагування на інциденти, служба підтримки, відділ безпеки або відділ з питань приватності. Якщо організаціям заборонено переглядати та аналізувати записи аудиту або вони не можуть здійснювати таку діяльність, перегляд або аналіз можуть здійснювати інші організації, яким надано такі повноваження. Обсяг, частота та/або детальність перевірки, аналізу та звітування за результатами аудиту можуть бути скориговані відповідно до потреб організації на основі нової інформації, що надходить до неї. Зіставлення процесів перевірки, аналізу та звітності допомагає гарантувати, що вони в сукупності створюють більш повне уявлення про події. Вимога до оцінки певної системи не залежить від того, чи

№	Назва вимоги	Опис вимоги
		застосовується таке зіставлення на рівні системи, чи на рівні організації в усіх системах.
3.6.	Скорочення записів аудиту та формування звіту	Записи аудиту генеруються в 3.3. Після створення запису аудиту виконується скорочення запису аудиту та формування звіту. Скорочення записів аудиту – це процес, який маніпулює зібраною інформацією аудиту та організовує таку інформацію в узагальненому форматі, який є більш значущим для аналітиків. Можливості скорочення записів аудиту та створення звітів не завжди походять від однієї системи або структур організації, що здійснюють діяльність аудиту. Функція скорочення записів аудиту може включати, наприклад, сучасні методи інтелектуального аналізу даних з розширеними фільтрами даних для виявлення аномальної поведінки в записах аудиту. Можливості формування записів, що надаються системою, можуть допомогти у створенні звітів, що налаштовуються. Впорядкування записів аудиту за часом може бути суттєвою проблемою, якщо деталізація позначки часу в записі є недостатньою.
3.7.	Позначка часу	Внутрішні годинники в системах використовуються для генерації позначок часу, які включають дату та час. Час виражається у Всесвітньому координованому часі (UTC), середнього часу за Гринвічем (GMT), або місцевому часі зі зміщенням від UTC. Точність вимірювання часу відноситься до ступеня синхронізації між годинником в системі та еталонним годинником, наприклад, годинник, що синхронізується в межах сотень мілісекунд або в межах десятків мілісекунд. Організації можуть визначати різну деталізацію часу для різних компонентів системи. Служба часу також може бути критично важливою для інших можливостей безпеки, таких як контроль доступу, ідентифікація та автентифікація, в залежності від характеру механізмів, що використовуються для підтримки цих можливостей.
3.8.	Захист інформації аудиту	Інформація аудиту включає всю інформацію (наприклад, записи аудиту, налаштування журналу аудиту та звіти аудиту), необхідну для успішного проведення аудиту діяльності системи. Інструменти реєстрації записів аудиту – це програми та пристрої, що використовуються для проведення аудиту та реєстрації записів аудиту. Ця вимога зосереджена на технічному захисті інформації аудиту та обмежує можливість доступу до інструментів реєстрації аудиту та їх використання лише авторизованими особами. Фізичний захист інформації аудиту забезпечується вимогами щодо захисту носіїв інформації та фізичного захисту. Особи або ролі з привілейованим доступом до системи, які також є об'єктом аудиту цієї системи, можуть впливати на достовірність інформації аудиту, перешкоджаючи веденню журналів аудиту або змінюючи записи аудиту. Ця вимога визначає, що привілейований

№	Назва вимоги	Опис вимоги
		доступ слід розмежовувати між привілеями, пов'язаними з аудитом, та іншими привілеями, обмежуючи таким чином коло користувачів, які мають привілеї, пов'язані з аудитом.
4.	**Управління конфігурацією**	
4.1.	Базова конфігурація	Базові конфігурації системи та компонентів системи включають аспекти підключення, експлуатації та комунікації. Базові конфігурації - це задокументовані, підтвердженні та узгоджені специфікації для системи або елементів конфігурації в системі. Базові конфігурації слугують основою для майбутніх збірок, випусків або змін у системі і включають інформацію про компоненти системи, операційні процедури, топологію мережі та розміщення компонентів в архітектурі системи. Підтримка базових конфігурацій вимагає створення нових базових конфігурацій у міру того, як система змінюється з часом. Базові конфігурації системи відображають поточну архітектуру системи у визначений момент часу.
4.2.	Налаштування конфігурації	Параметри конфігурації - це набір параметрів, які можна змінювати в апаратних, програмних або програмно-апаратних компонентах системи і які впливають на стан безпеки або функціональність системи. Конфігураційні налаштування, пов'язані з безпекою, можна визначити для обчислювальних систем (наприклад, серверів, робочих станцій), пристроїв введення та виведення (наприклад, сканерів, копіювальних апаратів, принтерів), мережевих компонентів (наприклад, брандмауерів, маршрутизаторів, шлюзів, комутаторів голосу та даних, бездротових точок доступу, мережевих пристроїв, датчиків), операційних систем, проміжного програмного забезпечення та застосунків. Параметри безпеки - це параметри, які впливають на стан безпеки системи, включно з параметрами, необхідними для задоволення інших вимог безпеки. Параметри безпеки включають налаштування реєстру; налаштування дозволів для облікових записів, файлів і каталогів (тобто привілеїв); а також налаштування функцій, портів, протоколів і віддалених з'єднань. Організації встановлюють загальноорганізаційні параметри конфігурації, а потім виводять специфічні параметри конфігурації для системи. Встановлені параметри стають частиною базової конфігурації системи. Типові безпечні конфігурації (також відомі як контрольні списки конфігурації безпеки, посібники з блокування та захисту, довідники з безпеки та посібники з технічного впровадження безпеки) містять визнані, стандартизовані та встановлені еталони, які визначають параметри безпечної конфігурації для конкретних інформаційних платформ/продуктів, а також інструкції з налаштування цих

№	Назва вимоги	Опис вимоги
		компонентів системи відповідно до експлуатаційних вимог. Загальні безпечні конфігурації можуть розроблятися різними організаціями, включаючи розробників інформаційних технологій, виробників, постачальників та інших організацій в державному та приватному секторах.
4.3.	Управління змінами конфігурації	Контроль змін конфігурації - це відстеження, перевірка, схвалення або несхвалення та реєстрація змін у системі. Зокрема, він включає пропозицію змін до системи, обґрунтування, впровадження, тестування, перевірку та затвердження змін до системи, в тому числі оновлення та модифікацію системи. Контроль змін конфігурації включає зміни базових конфігурацій компонентів системи (наприклад, операційних систем, додатків, брандмауерів, маршрутизаторів, мобільних пристроїв) та елементів конфігурації системи, зміни налаштувань конфігурації, незаплановані та несанкціоновані зміни, а також зміни, спрямовані на усунення вразливостей.
4.4.	Аналіз впливу на безпеку та приватність	Персонал організації, відповідальний за безпеку, проводить аналіз впливу, який включає перегляд планів, політик і процедур безпеки для розуміння вимог безпеки; перегляд проектної документації та операційних процедур системи для розуміння того, як зміни в системі можуть вплинути на стан безпеки системи; перегляд впливу змін на партнерів у ланцюгу постачання разом із зацікавленими сторонами; визначення того, як потенційні зміни в системі створюють нові ризики, а також можливості зменшити ці ризики. Аналіз впливу також включає оцінку ризиків, щоб зрозуміти наслідки змін і визначити, чи потрібні додаткові вимоги до безпеки.
4.5.	Обмеження доступу до змін	Зміни в апаратних, програмних або мікропрограмних компонентах системи або в операційних процедурах, пов'язаних із системою, можуть мати потенційно значний вплив на безпеку системи. Тому організації дозволяють лише кваліфікованим та уповноваженим особам отримувати доступ до системи з метою ініціювання змін. Обмеження доступу включають фізичні та логічні засоби контролю доступу, програмні бібліотеки, автоматизацію робочих процесів, абстрактні рівні (тобто зміни, що вносяться у зовнішні інтерфейси, а не безпосередньо в систему) та вікна змін (тобто зміни відбуваються лише у визначений час).
4.6.	Мінімально необхідна функціональність	Системи можуть надавати різноманітні функції та послуги. Деякі функції та послуги, які надаються за замовчуванням, можуть не бути необхідними для підтримки основних завдань організації, функцій або операцій. Може бути зручно надавати кілька послуг з одного компонента системи. Однак це збільшує ризик через обмеження послуг, що надаються будь-яким одним компонентом. Там, де це можливо, організації обмежують функціональність до однієї функції на компонент.

№	Назва вимоги	Опис вимоги
		Організації переглядають функції та послуги, що надаються системою або компонентами системи, щоб визначити, які функції та послуги є кандидатами на усунення. Організації відключають невикористовувані або непотрібні фізичні та логічні порти і протоколи, щоб запобігти несанкціонованому підключенню пристроїв, передачі інформації та тунелюванню. Організації можуть використовувати інструменти мережевого сканування, системи виявлення та запобігання вторгненням і системи захисту кінцевих точок (наприклад, брандмауери та системи виявлення вторгнень на основі хостів) для виявлення та запобігання використанню заборонених функцій, портів, протоколів, з'єднань системи і сервісів. Bluetooth, протокол передачі файлів і однорангові мережі є прикладами типів протоколів, які організації розглядають для усунення, обмеження або відключення.
4.7.	Мінімально необхідна функціональність – авторизоване програмне забезпечення – чорний список	За наявності необхідних привілеїв користувачі можуть встановлювати програмне забезпечення в системах організації. Щоб підтримувати контроль над встановленим програмним забезпеченням, організації визначають дозволені та заборонені дії щодо встановлення програмного забезпечення. Дозволене встановлення програмного забезпечення включає оновлення та виправлення безпеки для існуючого програмного забезпечення та завантаження нових програм зі схвалених організацією "магазинів програм". До заборонених програм належать програми з невідомим або підозрілим походженням, а також програми, які організація вважає потенційно шкідливими. Політики, обрані для управління встановленим користувачем програмним забезпеченням, розробляються організацією або надаються зовнішніми суб'єктами. Методи застосування політик можуть включати процедурні та автоматизовані методи. Авторизовані програми можуть бути обмежені конкретними версіями або походити з конкретного джерела. Щоб полегшити комплексний процес перевірки авторизованого програмного забезпечення та підвищити надійність захисту від атак, які обходять авторизоване програмне забезпечення на рівні додатків, програмне забезпечення може бути розбите на різні рівні деталізації та відстежуватися на різних рівнях. Ці рівні включають програми, інтерфейси прикладних програм, модулі програм, сценарії, процеси системи, служби системи, функції ядра, реєстри, драйвери та бібліотеки динамічних посилань. Організації розглядають можливість перевірки цілісності авторизованого програмного забезпечення за допомогою цифрових електронних підписів, криптографічних контрольних сум або хеш-функцій. Перевірка авторизованого програмного забезпечення може

№	Назва вимоги	Опис вимоги
		відбуватися або перед виконанням, або під час запуску системи.
4.8.	Інвентаризація компонентів системи	Компоненти системи - це окремі ідентифіковані активи (наприклад, апаратне забезпечення, програмне забезпечення та елементи програмного забезпечення), які складають систему. Організації можуть впроваджувати централізовані переліки компонентів системи, які включають компоненти з усіх систем. У таких ситуаціях організації забезпечують, щоб перелік включав специфічну для системи інформацію, необхідну для звітування про компоненти. Інформація, необхідна для ефективного обліку компонентів системи, включає назву системи, власників програмного забезпечення, номери версій програмного забезпечення, інвентаризаційні специфікації обладнання, інформацію про ліцензії на програмне забезпечення, а для мережевих компонентів - назви комп'ютерів та мережеві адреси для всіх впроваджених протоколів (наприклад, IPv4, IPv6). Інвентаризаційні специфікації включають тип компонента, фізичне місцезнаходження, дату отримання, виробника, вартість, модель, серійний номер та інформацію про постачальника.
4.9.	Розташування інформації	Визначення розташування інформації передбачає необхідність розуміння конкретних компонентів системи, де обробляється і зберігається інформація, а також користувачів, які мають доступ до інформації, щоб забезпечити відповідні механізми захисту, включаючи контроль інформаційних потоків, контроль доступу та управління інформацією.
4.10.	Базова конфігурація – конфігурація системи та компонентів для сфер з високим ризиком	Якщо відомо, що система або певний компонент системи перебуватиме в зоні підвищеного ризику, можуть знадобитися додаткові вимоги до безпеки, щоб протистояти підвищеній загрозі. Організації можуть впроваджувати захисні заходи щодо системи або компонентів системи, якими користуються особи, що виїжджають у відрядження та повертаються з них. Заходи включають визначення місць, які викликають занепокоєння, визначення необхідних конфігурацій для компонентів, забезпечення того, щоб компоненти були налаштовані належним чином до початку подорожі, а також вжиття додаткових заходів після завершення відрядження. Наприклад, системи, що відправляються в зони підвищеного ризику, можуть бути сконфігуровані з очищеними жорсткими дисками, обмеженим набором програмного забезпечення та більш посиленими налаштуваннями конфігурації безпеки. Дії, що застосовуються до мобільних пристроїв після повернення з відрядження, включають перевірку пристрою на наявність ознак фізичного втручання, а також очищення та перезапис пам'яті пристрою.

№	Назва вимоги	Опис вимоги
5.	**Ідентифікація та автентифікація**	
5.1.	Ідентифікація та автентифікація (користувачів організації)	Користувачами системи є особи (або процеси системи, що діють від імені осіб), які мають право доступу до системи. Як правило, індивідуальними ідентифікаторами є імена користувачів, пов'язані з обліковими записами в системі, призначеними цим особам. Оскільки процеси в системі виконуються від імені груп і ролей, організації можуть вимагати унікальної ідентифікації осіб у групових облікових записах або для обліку індивідуальної активності. Унікальна ідентифікація та автентифікація користувачів застосовується до всіх доступів до системи. Організації використовують паролі, фізичні автентифікатори, біометричні дані або їх комбінацію для автентифікації користувачів. Організації можуть повторно автентифікувати осіб у певних ситуаціях, зокрема, коли змінюються ролі, автентифікатори чи облікові дані; коли відбувається виконання привілейованих функцій; через певний проміжок часу або періодично.
5.2.	Ідентифікація та автентифікація пристроїв	Пристрої, які потребують унікальної ідентифікації та автентифікації від пристрою до пристрою, визначаються за типом, пристроєм або комбінацією типу та пристрою. Типи пристроїв, визначені організацією, включають пристрої, які не належать організації. Системи використовують загальновідому інформацію (наприклад, Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP]) для ідентифікації пристроїв або рішення для автентифікації організації (наприклад, протокол Institute of Electrical and Electronics Engineers [IEEE] 802.1x і Extensible Authentication Protocol [EAP], сервер RADIUS з автентифікацією на EAP-Transport Layer Security [TLS], Kerberos) для ідентифікації та автентифікації пристроїв у локальних і глобальних мережах. Інфраструктура відкритих ключів (PKI) і перевірка відкликання для обмінюваних сертифікатів також можуть бути включені як частина автентифікації пристрою.
5.3.	Ідентифікація та автентифікація (користувачів організації) – багатофакторна автентифікація привілейованих облікових записів	Багатофакторна автентифікація вимагає використання двох або більше різних факторів для досягнення автентифікації. Фактори автентифікації визначаються наступним чином: щось, що знайоме користувачу (наприклад, персональний ідентифікаційний номер [PIN-код]), щось, що має користувач (наприклад, фізичний автентифікатор, наприклад, криптографічний особистий ключ), або щось, властиве фізичній особі (наприклад, біометричні дані). Рішення для багатофакторної автентифікації, які використовують фізичні автентифікатори, включають апаратні автентифікатори, які надають результати на основі часу або виклику-відповіді, а також смарт-карти. Окрім автентифікації користувачів на рівні системи, організації також можуть використовувати механізми автентифікації

№	Назва вимоги	Опис вимоги
		на рівні програм для забезпечення підвищеного рівня інформаційної безпеки.
5.4.	Ідентифікація та автентифікація (користувачів організації) – доступ до облікових записів – стійкість до відтворення	Процеси автентифікації протидіють атакам повторного відтворення, якщо неможливо успішно автентифікуватись шляхом запису або повторного відтворення попередніх автентифікаційних повідомлень. Методи, стійкі до повторного відтворення, включають протоколи, які використовують одноразові номери або виклики, такі як синхронізовані за часом або одноразові автентифікатори "виклик-відповідь".
5.5.	Управління ідентифікацією	Ідентифікатори надаються користувачам, процесам, що діють від імені користувачів, або пристроям. Запобігання повторному використанню ідентифікаторів передбачає запобігання присвоєнню раніше використаних ідентифікаторів особи, групи, ролі, сервісу або пристрою різним особам, групам, ролям, сервісам або пристроям. До характеристик, які ідентифікують статус фізичних осіб, належать підрядники, іноземні громадяни та неорганізаційні користувачі. Ідентифікація статусу осіб за цими характеристиками надає важливу інформацію про людей, з якими спілкується персонал організації. Наприклад, працівнику важливо знати, що один із співрозмовників в електронному листі є підрядником.
5.6.	Управління автентифікатором – автентифікація на основі пароля	Дана вимога застосовується до паролів, що використовуються в однофакторній або багатофакторній автентифікації. Довгі паролі або парольні фрази є кращими, ніж короткі паролі. Правила обов'язкового створення паролів дають незначні переваги у безпеці, але зменшують зручність використання. Однак організації можуть встановити певні правила для створення паролів (наприклад, мінімальну довжину символів) за певних обставин та можуть забезпечити дотримання цієї вимоги. Наприклад, відновлення облікового запису може відбуватися, коли пароль забувається. Криптографічно захищені паролі включають односторонні криптографічні хеші паролів. Список часто використовуваних, скомпрометованих або очікуваних паролів включає паролі, отримані з попередніх баз даних про зломи, слова зі словників, а також повторювані або послідовні символи. До списку входять слова, що залежать від контексту, такі як назва сервісу, ім'я користувача та похідні від них. Зміна тимчасових паролів на постійні відразу після входу в систему гарантує, що необхідна надійність механізму автентифікації буде реалізована при першій же можливості, і знижує вразливість до компрометації автентифікатора. Для підвищення складності паролів можна використовувати довгі паролі та кодові фрази.

№	Назва вимоги	Опис вимоги
5.7.	Зворотний зв'язок автентифікатора	Зворотний зв'язок від систем не надає інформації, яка б дозволила неавторизованим особам скомпрометувати механізми автентифікації. Наприклад, для стаціонарних комп'ютерів або ноутбуків з відносно великими моніторами ця загроза може бути значною (її часто називають " Плечовий серфінг "). Для мобільних пристроїв з невеликими дисплеями ця загроза може бути менш значущою але збільшується через підвищену ймовірністю помилок введення через маленькі клавіатури. Тому засоби для приховування зворотного зв'язку з автентифікатором обираються відповідні. Приховування зворотного зв'язку включає в себе відображення зірочок, коли користувачі вводять паролі на пристроях введення, або відображення зворотного зв'язку протягом обмеженого часу, перш ніж повністю його приховати.
5.8.	Управління автентифікатором	До автентифікаторів належать паролі, криптографічні засоби, біометричні дані, сертифікати, пристрої з одноразовими паролями та ідентифікаційні значки. Початковий вміст автентифікатора - це фактичний вміст автентифікатора (наприклад, початковий пароль). На відміну від цього, вимоги до вмісту автентифікатора містять специфічні характеристики. Керування автентифікатором підтримується визначеними організацією налаштуваннями та обмеженнями для різних характеристик автентифікатора (наприклад, складність та правила складання паролів, часове вікно перевірки для синхронізованих у часі одноразових токенів та кількість дозволених відхилень на етапі верифікації біометричної автентифікації). Вимога щодо захисту індивідуальних автентифікаторів може бути реалізована до 15.3 для автентифікаторів, що знаходяться у володінні фізичних осіб, і до 1.1, 1.2, 1.5 та 13.4 для автентифікаторів, що зберігаються в системах організації. Сюди входять паролі, що зберігаються в хешованих або зашифрованих форматах, або файли, що містять зашифровані або хешовані паролі, до яких є доступ з правами адміністратора. Можна вжити заходів для захисту автентифікаторів, зокрема зберігати автентифікатори у себе, не передавати їх іншим особам і негайно повідомляти про втрачені, викрадені або скомпрометовані автентифікатори. Розробники можуть постачати компоненти системи з заводськими обліковими даними автентифікації за замовчуванням, щоб забезпечити початкове встановлення та конфігурацію. Облікові дані для автентифікації за замовчуванням часто добре відомі, їх легко знайти, і вони становлять значний ризик. Керування автентифікаторами включає видачу та відкликання автентифікаторів для тимчасового доступу, коли вони більше не потрібні. Використання довгих паролів або фраз

№	Назва вимоги	Опис вимоги
		може позбавити від необхідності періодичної зміни автентифікаторів.
6.	**Реагування на інциденти**	
6.1.	Обробка інциденту	Важливо, щоб організації розробляли та впроваджували скоординований підхід до реагування на інциденти. Ціль організації та її функції визначають структуру можливостей реагування на інциденти. Інформація про інциденти може бути отримана з різних джерел, включаючи аудит, моніторинг мережі, моніторинг фізичного доступу, звіти користувачів та адміністраторів, а також звіти від постачальників програмного забезпечення. Ефективна система реагування на інциденти передбачає координацію між багатьма підрозділами організації, в тому числі власників інформації, власниками систем, відділами кадрів, відділами фізичної та кадрової безпеки, юридичними відділами, оперативним персоналом та відділами закупівель.
6.2.	Моніторинг інциденту	Документування інцидентів включає ведення записів про кожен інцидент, статус інциденту та іншу відповідну інформацію, необхідну для проведення аналізу, а також оцінки деталей інциденту, тенденцій та обробки. Інформація про інциденти може бути отримана з багатьох джерел, включаючи моніторинг мережі, звіти про інциденти, групи реагування на інциденти, скарги користувачів, постачальників, моніторинг аудиту, моніторинг фізичного доступу, звіти користувачів/адміністраторів. 6.1 надає інформацію про типи інцидентів, які підходять для моніторингу. Типи інцидентів, про які повідомляється, зміст та своєчасність звітів, а також органи, що відповідають за звітність, відповідають чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам та керівним принципам. Інформація про інциденти використовується для оцінювання ризиків, ефективності оцінювання безпеки, вимог безпеки до закупівель та критеріїв вибору технологічних продуктів. Ресурси підтримки реагування на інциденти, що надаються організаціями, включають служби підтримки, групи допомоги, автоматизовані системи для відкриття та відстеження заявок на реагування на інциденти, а також доступ до експертних послуг.
6.3.	Перевірка реагувань на інциденти	Організації тестують можливості реагування на інциденти, щоб визначити їхню ефективність і виявити потенційні слабкі місця або недоліки. Тестування реагування на інциденти включає в себе використання контрольних списків, покрокові або групові вправи, а також симуляції. Тестування реагування на інциденти може включати

№	Назва вимоги	Опис вимоги
		визначення впливу реагування на інцидент на діяльність організації, її активи та окремих осіб. Якісні та кількісні дані можуть допомогти визначити ефективність процесів реагування на інциденти.
6.4.	Навчання з реагування на інциденти	Навчання з реагування на інциденти пов'язане з призначеними ролями та обов'язками персоналу організації, що забезпечує відповідний зміст та рівень деталізації такого навчання. Наприклад, користувачам може бути достатньо знати, кому телефонувати або як розпізнати інцидент; адміністраторам системи може знадобитися додаткова підготовка з обробки інцидентів; а фахівці з реагування на інциденти можуть отримати спеціальну підготовку з експертизи, методів збору даних, звітності, відновлення системи. Навчання з реагування на інциденти включає в себе навчання користувачів щодо виявлення та повідомлення про підозрілі дії із зовнішніх та внутрішніх джерел. Підготовка користувачів з реагування на інциденти може бути надана в рамках 2.2. Події, які можуть прискорити оновлення змісту навчання з реагування на інциденти, включають тестування плану реагування на інциденти, реагування на фактичний інцидент, результати аудиту або оцінки, а також зміни в чинному законодавстві, виконавчих наказах, політиках, директивах, положеннях, стандартах і настановах.
7.	**Технічне обслуговування**	
7.1.	Інструменти для обслуговування	Затвердження, контроль, моніторинг та перегляд інструментів технічного обслуговування вирішують питання безпеки, пов'язані з інструментами, які використовуються для діагностики та ремонту системи. Інструменти технічного обслуговування можуть включати апаратне та програмне діагностичне і тестове обладнання, а також перехоплювачі пакетів. Інструменти можуть бути попередньо встановленими, принесеними з технічним персоналом на носіях, хмарними або завантаженими з веб-сайту. Діагностичні та тестові програми є потенційними засобами для навмисного або ненавмисного перенесення шкідливого коду в систему. Приклади перевірки носіїв включають перевірку криптографічного хешу або електронних підписів діагностичних і тестових програм та/або носіїв. Якщо організація перевіряє носії, які містять діагностичні та тестові програми, і виявляє, що вони також містять шкідливий код, інцидент обробляється відповідно до політики та процедур обробки інцидентів. Періодична перевірка засобів обслуговування може призвести до відкликання схвалення застарілих, непідтримуваних, неактуальних або таких, що більше не використовуються, засобів. Інструменти технічного обслуговування не

№	Назва вимоги	Опис вимоги
		стосуються апаратних і програмних компонентів, які підтримують технічне обслуговування і вважаються частиною системи (включаючи програмне забезпечення, що реалізує такі утиліти, як "ping", "ls", "ipconfig", або апаратне і програмне забезпечення, що реалізує порт моніторингу комутатора Ethernet).
7.2.	Віддалене обслуговування	Віддалене технічне обслуговування та діагностика проводяться особами, які комунікують через зовнішню або внутрішню мережу. Локальне технічне обслуговування та діагностика виконуються особами, які фізично присутні в місці розташування системи і не спілкуються через мережеве з'єднання. Методи автентифікації, що використовуються для створення віддалених сеансів технічного обслуговування та діагностики, відповідають вимогам 5.1.
7.3.	Технічний персонал	Персонал з технічного обслуговування відноситься до осіб, які виконують технічне обслуговування апаратного або програмного забезпечення системи, в той час як 10.1 стосується фізичного доступу для осіб, чиї обов'язки з технічного обслуговування дозволяють їм перебувати в межах периметру фізичного захисту системи. Технічна компетенція осіб, які здійснюють нагляд, відноситься до технічного обслуговування, що виконується в системі, тоді наявність необхідних дозволів на доступ відноситься до технічного обслуговування в системі та поблизу неї. Особи, які раніше не були визначені як уповноважений обслуговуючий персонал (наприклад, виробники, консультанти, інтегратори системи та постачальники), можуть потребувати привілейованого доступу до системи, наприклад, коли їм потрібно провести технічне обслуговування без попереднього повідомлення або взагалі без нього. Організації можуть прийняти рішення про видачу тимчасових повноважень цим особам на основі оцінки ризиків. Тимчасові повноваження можуть бути одноразовими або на дуже обмежений період часу.
8.	**Захист носіїв інформації**	
8.1.	Зберігання носіїв інформації	Носії інформації включають цифрові та нецифрові носії. До цифрових носіїв належать дискети, флеш-накопичувачі, магнітні стрічки, зовнішні та знімні жорсткі диски, компакт-диски та цифрові відеодиски. Нецифрові носії включають папір і мікроплівка. Фізичний контроль за носіями інформації, що зберігаються, включає проведення інвентаризації, встановлення процедур, що дозволяють користувачам отримувати і повертати носії інформації до сховищ, а також ведення звітності за носії інформації, що зберігаються. Безпечне зберігання включає замкнений ящик, стіл або шафу, або контрольоване місце зберігання. Контрольовані зони забезпечують фізичний і процедурний контроль, щоб відповідати вимогам, встановленими для

№	Назва вимоги	Опис вимоги
		захисту інформації та систем. Методи очистки (наприклад, криптографічне стирання, очищення та знищення) запобігають розкриттю службової інформації несанкціонованим особам. Процес очищення видаляє службову інформацію з носіїв інформації таким чином, щоб її неможливо було відновити або реконструювати.
8.2.	Доступ до носіїв інформації	Носії інформації включають цифрові та нецифрові носії. Доступ до інформації на носіях інформації можна обмежити шляхом фізичного контролю таких носіїв інформації, що включає проведення інвентаризації, забезпечення наявності процедур, які дозволяють особам брати та повертати носії інформації до сховищ, а також ведення обліку носіїв інформації, що зберігаються.
8.3.	Знищення інформації на носіях інформації	Очищення носіїв інформації застосовується до цифрових і нецифрових носіїв інформації, які підлягають утилізації або повторному використанню, незалежно від того, чи вважаються ці носії інформації знімними чи ні. Приклади включають цифрові носії інформації в сканерах, копірах, принтерах, ноутбуках, робочих станціях, мобільних пристроях, мережевих компонентах і нецифрових носіях. В процесі очищення інформації з носіїв, інформація не може бути відновлена або реконструйована. Методи очищення (наприклад, криптографічне стирання, очищення та знищення) запобігають розголошенню інформації несанкціонованим особам, коли такі носії інформації повторно використовуються або передаються на утилізацію. Процес очищення носіїв інформації, або їх знищення, встановлюється нормативно-правовими актами щодо обробки інформації.
8.4.	Маркування носіїв інформації	Носії інформації включають цифрові та нецифрові носії. Маркування - це нанесення або використання атрибутів безпеки, які зчитуються людиною. Маркування означає використання атрибутів безпеки для внутрішніх структур даних системи. До цифрових носіїв належать дискети, флеш-накопичувачі, магнітні стрічки, зовнішні та знімні жорсткі диски, компакт-диски та цифрові відеодиски. Нецифрові носії включають папір і мікроплівки. Визначення службової інформації разом із вимогами до маркування, захисту та розповсюдження такої інформації встановлюється нормативно-правовими актами щодо обробки службової інформації
8.5.	Транспортування носіїв інформації	Носії інформації включають цифрові та нецифрові носії. До цифрових носіїв належать дискети, флеш-накопичувачі, магнітні стрічки, зовнішні та знімні жорсткі диски, компакт-диски та цифрові відеодиски. Нецифрові носії включають папір і мікроплівки. Контрольовані зони - це території, для яких організації забезпечують фізичні або процедурні заходи для виконання вимог, встановлених для захисту інформації та систем. Захист носіїв інформації під час транспортування може включати використання

№	Назва вимоги	Опис вимоги
		криптографії та/або замкнених контейнерів. Криптографічні механізми можуть забезпечувати захист конфіденційності, залежно від застосованих механізмів. Діяльність, пов'язана з транспортуванням носіїв інформації, включає підготовку носіїв інформації до транспортування, забезпечення того, щоб носії інформації потрапили до відповідних транспортних процесів, і власне транспортування. Уповноважений транспортний і кур'єрський персонал може включати осіб, які не є співробітниками організації. Забезпечення контролю за носіями інформації під час транспортування включає в себе обмеження транспортних операцій уповноваженим персоналом, а також відстеження або отримання записів про транспортні операції під час проходження носія інформації через транспортну систему з метою запобігання та виявлення втрат, знищення або фальсифікацій. Ця вимога пов'язана з 13.7.
8.6.	Використання носіїв інформації	На відміну від вимоги 8.1, яка обмежує доступ користувача до носіїв інформації, ця вимога обмежує використання певних типів носіїв інформації, наприклад, обмежує або забороняє використання зовнішніх жорстких дисків, флеш-накопичувачів або смарт-карт Ця вимога також включає будь-які потенційні обмеження на використання знімних носіїв інформації у зовнішніх системах. Організації можуть використовувати технічні та нетехнічні заходи (наприклад, політики, процедури та правила поведінки) для контролю використання носіїв інформації. Наприклад, організації можуть контролювати використання портативних пристроїв зберігання даних, встановлюючи на робочих станціях фізичні обмеження доступу до зовнішніх портів або вимикаючи чи вилучаючи можливість вставляти, читати чи записувати на пристрої. Організації можуть обмежити використання портативних носіїв інформації лише дозволеними носіями інформації, включаючи носії інформації, надані організацією, носії інформації, надані іншими дозволеними організаціями, а також носії інформації, які не перебувають в особистій власності. Організації також можуть контролювати використання портативних носіїв інформації на основі типу носія інформації - забороняти використання портативних носіїв інформації, які можна записувати - і впроваджувати це обмеження шляхом вимкнення або видалення можливості записувати на такі носії інформації. Обмеження на використання носіїв інформації, контрольованих організацією, у зовнішніх системах включають обмеження на те, як ці носії можуть використовуватися та за яких умов. Вимога щодо ідентифікації власників знімних носіїв інформації (наприклад, фізичних осіб, організацій чи проектів) знижує ризик використання таких технологій, оскільки дозволяє організаціям розподіляти

№	Назва вимоги	Опис вимоги
		відповідальність та підзвітність за усунення відомих вразливостей у носіях інформації (наприклад, вставки шкідливого коду).
8.7.	Резервне копіювання - криптографічний захист	Місця зберігання резервних копій можуть включати інформацію рівня системи та інформацію рівня користувача. Інформація рівня системи включає інформацію про стан системи, програмне забезпечення операційної системи, прикладне програмне забезпечення та ліцензії. До інформації на рівні користувача належить інформація, відмінна від інформації на рівні системи. Апаратні технології безпеки (наприклад, апаратні модулі безпеки [HSM]) можна використовувати для посилення криптографічного захисту резервної інформації. Пристрої HSM захищають криптографічні ключі та керують ними, а також забезпечують криптографічну обробку. Криптографічні операції (наприклад, шифрування, дешифрування та генерація/перевірка підписів) зазвичай виконуються на пристрої HSM, і багато реалізацій надають механізми апаратного прискорення для криптографічних операцій. Ця вимога пов'язана з 13.7.
9.	**Кадрова безпека**	
9.1.	Перевірка персоналу	Заходи з безпеки по перевірці персоналу передбачають оцінку поведінки, доброчесності, лояльності, надійності та стабільності (тобто ступеня довіри до особи) перед тим, як надати доступ до системи або підвищити рівень доступу до системи. Діяльність з перевірки та повторної перевірки відповідає чинному законодавству, виконавчим наказам, директивам, політикам, положенням і критеріям, встановленим для рівня доступу, необхідного для призначеної посади.
9.2.	Звільнення персоналу. Переведення персоналу	Обладнання системи, пов'язане з безпекою, включає токени автентифікації обладнання, технічні посібники з адміністрування системи, ключі, ідентифікаційні картки та перепустки до будівлі. Співбесіди при звільненні гарантують, що особи, які звільняються, розуміють обмеження безпеки, що накладаються на них як на колишніх працівників, а також те, що вони несуть відповідальність за майно організації. Теми безпеки під час співбесідах при звільнені включають нагадування особам про потенційні обмеження щодо майбутнього працевлаштування та угоди про нерозголошення. Своєчасне виконання дій зі звільнення має важливе значення для осіб, які звільняються за власним бажанням. Організації можуть розглянути можливість блокування облікових записів осіб, які звільняються, до того, як вони будуть повідомлені про це. Ця вимога застосовується до перепризначення або переведення осіб, коли кадрові зміни є постійними або такими тривалими, що потребують захисту. Заходи захисту, які можуть знадобитися при

№	Назва вимоги	Опис вимоги
		переведенні або призначенні на іншу посаду в організації, включають повернення старих і видачу нових ідентифікаційних карток, ключів і перепусток до будівлі; зміну дозволів на доступ до системи (тобто привілеїв); закриття облікових записів і створення нових; надання доступу до офіційних документів, до яких особи мали доступ на попередніх посадах за допомогою попередніх облікових записів у системі.
10.	**Фізичний захист і захист робочого середовища**	Об'єкт може включати в себе одне або кілька фізичних місць, що містять системи або компоненти системи, які обробляють, зберігають або передають службову інформацію. Дозволи на фізичний доступ поширюються на працівників і відвідувачів. Особи, які мають постійні облікові дані для фізичного доступу, не вважаються відвідувачами. До облікових даних авторизації належать ідентифікаційні бейджі, ідентифікаційні картки та смарт-картки. Організації визначають рівень авторизації відповідно до чинного законодавства, виконавчих наказів, директив, положень, політик, стандартів та інструкцій. Для доступу до певних зон на об'єктах, визначених як загальнодоступні, фізичні дозволи на доступ можуть не знадобитися.
10.1.	Авторизація фізичного доступу	Об'єкт може включати в себе одне або кілька фізичних місць, що містять системи або компоненти системи, які обробляють, зберігають або передають службову інформацію. Дозволи на фізичний доступ поширюються на працівників і відвідувачів. Особи, які мають постійні облікові дані для фізичного доступу, не вважаються відвідувачами. До облікових даних авторизації належать ідентифікаційні бейджі, ідентифікаційні картки та смарт-картки. Організації визначають рівень авторизації відповідно до чинного законодавства, виконавчих наказів, директив, положень, політик, стандартів та інструкцій. Для доступу до певних зон на об'єктах, визначених як загальнодоступні, фізичні дозволи на доступ можуть не знадобитися.
10.2.	Моніторинг фізичного доступу	Об'єкт може включати в себе одне або кілька фізичних місць, що містять системи або компоненти системи, які обробляють, зберігають або передають службову інформацію. Контроль фізичного доступу охоплює загальнодоступні зони в приміщеннях організації. Прикладами контролю фізичного доступу є: використання охоронців, обладнання для відеоспостереження (наприклад, камер) та сенсорних пристроїв. Перегляд журналів фізичного доступу може допомогти виявити підозрілу активність, аномальні події або потенційні загрози. Якщо журнали доступу є частиною автоматизованої системи, їх можна підтримувати за допомогою засобів контролю аудиту. Можливості реагування на інциденти включають розслідування

№	Назва вимоги	Опис вимоги
		інцидентів фізичної безпеки та реагування на них. Інциденти включають порушення безпеки або підозрілі дії з фізичним доступом, такі як доступ у неробочий час, повторний доступ до зон, до яких зазвичай немає доступу, доступ протягом незвично тривалого часу та позачерговий доступ.
10.3.	Альтернативне робоче місце	Альтернативні робочі місця включають особисті приміщення працівників або інші об'єкти, визначені організацією. Альтернативні робочі місця можуть забезпечити легкодоступні альтернативні місця під час надзвичайних ситуацій. Організації можуть визначати різні вимоги до безпеки для конкретних альтернативних робочих місць або типів місць, залежно від видів діяльності, пов'язаної з роботою, що проводиться на цих місцях. Оцінка ефективності вимог і забезпечення засобів повідомлення про інциденти на альтернативних робочих місцях допомагає організаціям у плануванні дій на випадок надзвичайних ситуацій.
10.4.	Керування фізичним доступом	Ця вимога стосується фізичних локацій, що містять системи або компоненти системи, які обробляють, зберігають або передають інформацію. Організації визначають, які типи охорони їм потрібні, зокрема професійні охоронці або адміністративний персонал. Пристрої фізичного доступу включають ключі, замки, комбінації, біометричні зчитувачі та зчитувачі карток. Системи контролю фізичного доступу відповідають чинному законодавству, виконавчим наказам, директивам, політикам, правилам, стандартам і настановам. Організації можуть гнучко використовувати різні типи журналів аудиту. Журнали аудиту можуть бути процедурними, автоматизованими або їх комбінацією. Фізичні точки доступу можуть включати зовнішні точки доступу, внутрішні точки доступу до систем, які потребують додаткового контролю доступу, або і ті, і інші. Контроль фізичного доступу застосовується до працівників та відвідувачів. Особи з постійними дозволами на фізичний доступ не вважаються відвідувачами.
10.5.	Контроль доступу до джерел і ліній електроживлення. Контроль доступу до пристроїв виведення інформації	Заходи захисту, що застосовуються до розподільчих ліній системи і ліній електропередач, запобігають випадковому пошкодженню, збоям і фізичному втручанню. Такі заходи також можуть бути необхідними для запобігання підслуховуванню або модифікації незашифрованих передач. Заходи захисту, що використовуються для контролю фізичного доступу до розподільчих і передавальних ліній системи, включають від'єднання або блокування запасних роз'ємів, замикання монтажних шаф, захист кабелів за допомогою кабелепроводів або кабельних лотків, а також датчики прослуховування. Контроль фізичного доступу до пристроїв виводу включає розміщення пристроїв виводу в замкнених приміщеннях або інших захищених зонах з контролем доступу за

№	Назва вимоги	Опис вимоги
		допомогою цифрової клавіатури або зчитувача карток і наданням доступу лише уповноваженим особам, розміщення пристроїв виводу в місцях, які можуть контролюватися персоналом, встановлення фільтрів на моніторах або екранах, що обмежують кути огляду, а також використання навушників. Прикладами пристроїв виведення є монітори, принтери, сканери, аудіо пристрої, факс і копіювальні апарати.
11.	**Оцінка ризику**	
11.1.	Оцінювання ризику	Встановлення меж системи є передумовою для оцінки ризику несанкціонованого розкриття службової інформації. Оцінка ризиків враховує загрози, вразливості, ймовірність та негативний вплив на діяльність та активи організації, пов'язані з функціонуванням і використанням системи та несанкціонованим розкриттям інформації. Оцінки ризиків також враховують ризики від зовнішніх сторін (наприклад, постачальників послуг, підрядників, які експлуатують системи від імені організації, осіб, які отримують доступ до систем). Оцінювання ризиків можна проводити на рівні організації, місії або бізнес-процесів, або на рівні системи, а також на будь-якому етапі життєвого циклу розробки системи. Оцінки ризиків включають ризики, пов'язані з ланцюгом постачання, що стосуються постачальників або підрядників та системи, компонента системи або послуги в системі, які вони надають.
11.2.	Сканування вразливостей	Організації визначають необхідний обсяг сканування вразливостей для компонентів системи та гарантують, що потенційні джерела вразливостей (наприклад, мережеві принтери, сканери та копіювальні апарати) не будуть проігноровані. Аналіз вразливостей для спеціального програмного забезпечення може вимагати додаткових підходів, таких як статичний аналіз, динамічний аналіз або бінарний аналіз. Організації можуть використовувати ці підходи в оглядах вихідного коду та інструментах (наприклад, інструментах статичного аналізу, сканерах додатків, бінарних аналізаторах). Сканування вразливостей включає сканування на предмет наявності встановлених оновлень; сканування функцій, портів, протоколів і служб, які не повинні бути доступними для користувачів або пристроїв; і сканування неправильно налаштованих або неправильно працюючих механізмів управління потоками. Щоб полегшити сумісність, організаціям слід розглянути можливість використання продуктів, які пройшли перевірку на відповідність протоколу Security Content Automated Protocol (SCAP) Автоматизований протокол безпеки даних і використовують Extensible Configuration ChecklistDescription Format (XCCDF). Організації також можуть розглянути можливість використання інструментів сканування, які описують вразливості відповідно до стандарту Common Vulnerabilities and Exposures (CVE).

№	Назва вимоги	Опис вимоги
		Поширені вразливості та ризики і використовують Open Vulnerability Assessment Language (OVAL). Джерела інформації про вразливості також включають список Common Weakness Enumeration (CWE), National Vulnerability Database (NVD) та Common Vulnerability Scoring System (CVSS).
12.	**Оцінювання, акредитація та моніторинг безпеки**	
12.1.	Оцінювання	Оцінюючи вимоги безпеки, організації визначають, чи правильно впроваджені необхідні засоби захисту та контрзаходи, чи працюють вони належним чином і чи дають бажаний результат. Оцінки безпеки виявляють слабкі місця та недоліки в системі та надають важливу інформацію, необхідну для прийняття рішень, що базуються на оцінці ризиків. Звіти з оцінки безпеки документують результати оцінки з такою деталізацією, яку організація вважає необхідною для визначення точності та повноти звітів. Результати оцінювання захищеності надаються особам або ролям, що відповідають типам оцінювання, які проводяться.
12.2.	План усунення недоліків та контрольні показники	План усунення недоліків є ключовим документом у програмі безпеки інформації. Організації можуть документувати план захисту інформації та план дій як окремі або об'єднані документи та в будь-якому обраному форматі. Уповноважені органи можуть розглядати надані План усунення недоліків системи як важливі вхідні дані для прийняття загального рішення щодо управління ризиками для обробки, зберігання або передачі конфіденційної інформації в системі, розміщеній в організації.
12.3.	Безперервний моніторинг	Безперервний моніторинг на рівні системи сприяє постійній обізнаності про стан безпеки системи для підтримки рішень з управління ризиками. Терміни "безперервний" і "постійний" означають, що організації оцінюють і контролюють свої системи з частотою, достатньою для підтримки рішень, заснованих на оцінці ризиків. Різні типи вимог безпеки можуть вимагати різної частоти моніторингу.
12.4.	Взаємодія систем	Вибір типів угод ґрунтується на таких факторах, як відносини між організаціями, що обмінюються інформацією (наприклад, уряд з урядом, уряд з бізнесом, бізнес з бізнесом, уряд або бізнес з постачальником послуг, уряд або бізнес з фізичною особою), а також рівень доступу до системи організації для користувачів іншої системи. Типи угод можуть включати угоди про безпеку з'єднання, угоди про безпеку обміну інформацією, меморандуми або угоди про взаєморозуміння, угоди про рівень обслуговування або інші типи угод. Організації можуть включати інформацію про угоди в офіційні контракти,

№	Назва вимоги	Опис вимоги
		особливо для обміну інформацією між державними установами та недержавними організаціями (наприклад, постачальниками послуг, підрядниками, розробниками систем та інтеграторами систем). Приклади типів інформації, що міститься в угодах про обмін, включають характеристики інтерфейсу, вимоги до безпеки, засоби контролю та обов'язки для кожної системи.
13.	**Захист інформаційної системи та комунікацій**	
13.1.	Захист периметра	Керовані інтерфейси включають шлюзи, маршрутизатори, брандмауери, мережеві системи аналізу та віртуалізації шкідливого коду або зашифровані тунелі, реалізовані в рамках архітектури безпеки системи. Підмережі, які фізично або логічно відокремлені від внутрішніх мереж, називаються демілітаризованими зонами або DMZ. Обмеження або заборона інтерфейсів в системах організації включає обмеження зовнішнього веб-трафіку до визначених веб-серверів в межах контрольованих інтерфейсів, заборону зовнішнього трафіку, який підміняє внутрішні адреси, і заборону внутрішнього трафіку, який підміняє зовнішні адреси.
13.2.	Інформація в загальних ресурсах системи	Запобігання несанкціонованій та ненавмисній передачі інформації за допомогою загальних ресурсів системи запобігає тому, щоб інформація, створена діями попередніх користувачів або ролей (або діями процесів, що діють від імені попередніх користувачів або ролей), була доступною поточним користувачам або ролям (або поточним процесам, що діють від імені поточних користувачів або ролей), які отримують доступ до загальних ресурсів системи після того, як ці ресурси були повернуті назад до системи. В інших контекстах контроль інформації у ресурсів системи називається повторним використанням об'єктів та захистом залишкової інформації. Ця вимога не стосується збереження інформації, яка відноситься до залишкового представлення даних, які були номінально видалені; прихованих каналів (у тому числі каналів зберігання або синхронізації), де загальні ресурси маніпулюються з метою порушення обмежень потоку інформації; або компонентів в системах, для яких існують лише окремі користувачі або ролі.
13.3.	Захист периметра - Відмова за замовчуванням - Дозвіл за винятком	Ця вимога застосовується до вхідного та вихідного мережевого трафіку на межі системи та у визначених точках всередині системи. Політика мережевого трафіку за принципом "заборонити все, дозволити лише за винятком" гарантує, що дозволені лише необхідні та схвалені з'єднання.

№	Назва вимоги	Опис вимоги
13.4.	Конфіденційність і цілісність передачі. Захист інформації у стані спокою	Ця вимога стосується внутрішніх і зовнішніх мереж та будь-яких компонентів системи, які можуть передавати інформацію, зокрема серверів, ноутбуків, настільних комп'ютерів, мобільних пристроїв, принтерів, копіювальних апаратів, сканерів, факсів та радіостанцій. Незахищені шляхи передачі даних можуть бути перехоплені та модифіковані. Шифрування захищає інформацію від несанкціонованого розкриття під час передачі та зберігання. Інформація в сховищі (тобто інформація в стані спокою) - це стан інформації, коли вона не перебуває в процесі обробки або транзиту і знаходиться на внутрішніх або зовнішніх пристроях зберігання даних, мережевих пристроях зберігання даних та базах даних. Захист інформації під час зберігання не зосереджується на типі пристрою зберігання або частоті доступу до нього, а скоріше на стані інформації. Ця вимога стосується 13.7.
13.5.	Відключення мережі	Ця вимога стосується як внутрішніх, так і зовнішніх мереж. Припинення мережевих з'єднань, пов'язаних з сеансами зв'язку, включає в себе вилучення пов'язаних з ними TCP/IP-адрес або пар портів на рівні операційної системи, або вилучення мережевих призначень на рівні застосунків, якщо декілька сеансів застосунків використовують одне мережеве з'єднання на рівні операційної системи. Періоди бездіяльності можуть встановлюватися організаціями і включати періоди часу за типом мережевого доступу або для конкретних мережевих підключень.
13.6.	Встановлення та управління криптографічними ключами	Встановлення та управління криптографічними ключами включає генерацію, розповсюдження, зберігання, доступ, заміну та знищення ключів. Криптографічні ключі можуть створюватися та управлятися за допомогою ручних процедур або автоматизованих механізмів, що підтримуються ручними процедурами. Організації виконують вимоги щодо створення та управління ключами відповідно до чинного законодавства, наказів, політик, директив, положень і стандартів, які визначають відповідні опції, рівні та параметри. Ця вимога стосується 13.7.
13.7.	Криптографічний захист	Криптографічний захист впроваджується відповідно до чинного законодавства, виконавчих наказів, директив, положень, політик, стандартів та інструкцій.
13.8.	Спільні обчислювальні пристрої та застосунки	Пристрої для спільної роботи включають дошки, мікрофони та камери. Індикація використання включає сповіщення користувачів (наприклад, спливаюче меню про те, що йде запис або що мікрофон увімкнено), коли пристрої для спільної роботи активовані. Не використовуються спеціальні системи відеоконференцій, які зазвичай потребують, щоб один з учасників зателефонував або з'єднався з іншою стороною для активації відеоконференції. Рішення для запобігання

№	Назва вимоги	Опис вимоги
		використанню пристроїв включають заглушки для веб-камер і кнопки для вимкнення мікрофонів.
13.9.	Мобільний код	Мобільний код включає в себе програми або частини програм, отримані з віддалених систем, передані через мережу і виконані на локальній системі без явного встановлення або виконання одержувачем. Рішення щодо використання мобільного коду в системі ґрунтується на потенційній можливості коду завдати шкоди системі у разі зловмисного використання. Технології мобільного коду включають Java-аплети, JavaScript, HTML5, VBScript і WebGL. Обмеження на використання та інструкції з впровадження застосовуються до вибору та використання мобільного коду, встановленого на серверах, а також мобільного коду, що завантажується та виконується на окремих робочих станціях та пристроях, включаючи ноутбуки, смартфони та смарт-пристрої. Політика та процедури щодо мобільного коду передбачають дії, спрямовані на запобігання розробці, придбанню та використанню неприйнятного мобільного коду в системі, включаючи вимогу електронного підпису мобільного коду надійним джерелом.
13.10.	Автентифікація сесії	Захистит автентифікації передбачає захист зв'язку на сеансовому рівні, а не на рівні пакетів. Такий захист створює підстави для впевненості на обох кінцях сеансу зв'язку в постійній ідентичності інших сторін і достовірності переданої інформації. Захист автентичності включає в себе захист від атак "зловмисника посередині", перехоплення сеансів і вставки неправдивої інформації в сеанси.
14.	**Цілісність системи та інформації**	
14.1.	Виправлення дефектів	Організації визначають системи, на які впливають відомі недоліки програмного забезпечення та вбудованих програм, включно з потенційними вразливостями, що виникають внаслідок цих недоліків, і повідомляють цю інформацію призначеному персоналу, відповідальному за інформаційну безпеку. Оновлення, що стосуються безпеки, включають патчі, пакети оновлень, "гарячі" виправлення та антивірусні сигнатури. Організації усувають недоліки, виявлені під час оцінювання безпеки, постійного моніторингу, реагування на інциденти та обробки помилок в системі. Організації можуть скористатися наявними ресурсами, такими як бази даних Common Weakness Enumeration (CWE) або Common Vulnerabilities and Exposures (CVE), для усунення недоліків, виявлених в системах організації. Періоди, визначені організацією для оновлення важливого для безпеки програмного забезпечення та вбудованих програм, можуть варіюватися

№	Назва вимоги	Опис вимоги
		залежно від різних факторів, включаючи критичність оновлення (тобто, серйозність вразливості, пов'язаної з виявленим недоліком). Деякі типи виправлення вразливостей можуть вимагати більше тестування, ніж інші типи виправлень.
14.2.	Захист від шкідливого коду	Вставки шкідливого коду відбуваються через використання вразливостей системи. Виявити шкідливий код можна за допомогою періодичного сканування системи та сканування файлів із зовнішніх джерел у режимі реального часу під час завантаження, відкриття або виконання файлів. Шкідливий код може потрапити в систему різними способами, зокрема через електронну пошту, Інтернет та портативні пристрої зберігання даних. До шкідливого коду належать віруси, хробаки, троянські та шпигунські програми. Шкідливий код може бути записано в різних форматах, міститися в стиснутих або прихованих файлах, або приховано у файлах за допомогою таких методів, як стеганографія. На додаток до вищезгаданих технологій, ефективним засобом запобігання виконанню шкідливого коду може бути повсюдне управління конфігурацією, комплексний контроль цілісності програмного забезпечення та програмне забезпечення для боротьби з його експлуатацією. Шкідливий код може бути присутнім у комерційному готовому програмному забезпеченні та програмному забезпеченні, створеному на замовлення, і може включати логічні бомби, бекдори та інші типи атак, які можуть вплинути на роботу організації та її функції.
14.3.	Попередження, рекомендації та директиви з безпеки	Існує багато загальнодоступних джерел попереджень та рекомендацій щодо безпеки систем, які генерують попередження та рекомендації з безпеки для підтримки обізнаності про ситуацію в організаціях. Постачальники програмного забезпечення, служби підтримки також можуть надавати попередження та рекомендації щодо безпеки. Дотримання директив з безпеки має важливе значення з огляду на критичний характер багатьох з цих директив і потенційні негайні негативні наслідки для діяльності та активів організації, окремих осіб, інших організацій і держави, якщо ці директиви не будуть виконані вчасно.
14.4.	Моніторинг системи	Моніторинг системи включає в себе зовнішній і внутрішній моніторинг. До зовнішнього моніторингу належить спостереження за подіями, що відбуваються на межі системи. Внутрішній моніторинг включає спостереження за подіями, що відбуваються всередині системи. Організації можуть здійснювати моніторинг системи, наприклад, спостерігаючи за реєстрацією аудиторських записів у режимі реального часу або за іншими аспектами системи, такими як моделі доступу, характеристики доступу та інші дії. Цілі моніторингу можуть керувати визначенням подій.

№	Назва вимоги	Опис вимоги
		Можливість моніторингу системи досягається за допомогою різноманітних інструментів і методів (наприклад, програмне забезпечення для моніторингу аудиторських записів, системи виявлення вторгнень, системи запобігання вторгненням, програмне забезпечення для захисту від шкідливого коду, інструменти сканування, програмне забезпечення для моніторингу мережі). Пріоритетні місця для розміщення пристроїв моніторингу включають вибрані місця по периметру та безпосередньо перед входом до серверних ферм, які підтримують критичні програми, що використовуються на керованих інтерфейсах системи. Детальність моніторингу зібраної інформації базується на цілях моніторингу організації та спроможності системи підтримувати такі цілі. З'єднання системи можуть бути мережевими, віддаленими або локальними. Мережеве з'єднання - це будь-яке з'єднання з пристроєм, який взаємодіє через мережу (наприклад, локальну мережу, Інтернет). Віддалене з'єднання - це будь-яке з'єднання з пристроєм, який взаємодіє через зовнішню мережу (наприклад, Інтернет). Мережеві, віддалені та локальні з'єднання можуть бути дротовими або бездротовими. Непритаманні або спроби неавторизованих дії або умови, пов'язані з вхідним і вихідним комунікаційним трафіком, включають внутрішній трафік, який вказує на наявність шкідливого коду в системі або розповсюдження його серед компонентів системи, спроби несанкціонованого експорту інформації або передачі сигналів до зовнішніх систем. Докази наявності шкідливого коду використовуються для ідентифікації потенційно скомпрометованої системи. Вимоги до моніторингу системи, в тому числі потреба в типах моніторингу системи, можуть згадуватися в інших вимогах.
14.5.	Управління та збереження інформації	Державні установи розглядають вимоги щодо зберігання даних для недержавних організацій. Зберігання інформації в недержавних системах після укладення контрактів або угод збільшує поверхню атаки на ці системи та ризик компрометації інформації.
15.	**Планування безпеки**	
15.1.	Політика та процедури планування безпеки	Ця вимога стосується політик і процедур захисту інформації. Політики та процедури сприяють забезпеченню безпеки і повинні відповідати кожній групі вимог до безпеки службової інформації. Політики можуть бути включені як частина загальної політики безпеки організації або представлені окремими політиками, які відповідають кожній групі вимог. Процедури описують, як реалізуються політики, і можуть бути спрямовані на особу або роль, яка є об'єктом процедури. Процедури можуть бути

№	Назва вимоги	Опис вимоги
		задокументовані в планах безпеки системи або в одному чи декількох окремих документах.
15.2.	Плани захисту інформації та персональних даних	План захисту інформації містять ключові характеристики системи, яка обробляє, зберігає та передає інформацію, а також способи захисту системи та інформації. Плани захисту інформації містять достатньо інформації для того, щоб забезпечити розробку та впровадження заходів, які однозначно відповідають намірам планів, а також для подальшого визначення ризиків, якщо план буде впроваджено належним чином. Плани захисту інформації можуть бути збіркою документів, включаючи документи, які вже існують. Ефективні плани захисту системи використовують посилання на політики, процедури та додаткові документи (наприклад, проектні специфікації), з яких можна отримати детальну інформацію. Це зменшує вимоги до документації, пов'язаної з програмами безпеки, та зберігає інформацію про безпеку в інших усталених управлінських чи операційних сферах, пов'язаних з архітектурою організації, життєвим циклом розробки системи, інженерією системи та закупівлею.
15.3.	Правила поведінки	Правила поведінки - це різновид вимог про доступ для користувачів системи. Організації розглядають правила поведінки для роботи зі службовою інформацією на основі індивідуальних ролей та обов'язків користувачів і розрізняють правила, що застосовуються до привілейованих користувачів, і правила, що застосовуються до звичайних користувачів.
16.	**Придбання систем та послуг**	
16.1.	Процес закупівель	Вимоги безпеки включають функціональні вимоги безпеки та вимоги до забезпечення безпеки. Функціональні вимоги безпеки зазвичай випливають із завдань або вимог організації, а також вимог, викладених у законах, нормативних актах, політиках і стандартах. Похідні вимоги можуть включати можливості, функції та механізми безпеки. Вимоги до забезпечення можуть включати процеси розробки, процедури, методології та докази діяльності з розробки та оцінки, які дають підстави для впевненості в тому, що необхідна функціональність реалізована і має необхідну надійність механізму. Вимоги до надійності механізму, пов'язані з такими можливостями, функціями та механізмами, включають ступінь правильності, повноту, стійкість до втручання або обходу та стійкість до прямої атаки з боку постачальника (розробника). Ця вимога пов'язана з 16.3 та 17.2.
16.2.	Компоненти системи, що не підтримуються	Підтримка компонентів системи включає виправлення програмного забезпечення, оновлення вбудованого програмного забезпечення, заміну деталей та контракти на

№	Назва вимоги	Опис вимоги
		технічне обслуговування. Прикладом непідтримуваних компонентів може бути ситуація, коли постачальники більше не надають виправлення для критично важливого програмного забезпечення або оновлення продуктів, що може призвести до того, що супротивник зможе використати слабкі місця або недоліки встановлених компонентів. Винятки щодо заміни непідтримуваних компонентів системи включають системи, які забезпечують критично важливі для завдань або роботи організації можливості, коли новіші технології недоступні або коли системи настільки ізольовані, що встановлення компонентів на заміну не є можливим варіантом. Альтернативні джерела підтримки спрямовані на забезпечення постійної підтримки компонентів системи, які більше не підтримуються оригінальними виробниками, розробниками або постачальниками, коли такі компоненти залишаються важливими для виконання завдань та функцій організації . За необхідності, організації можуть налагодити внутрішню підтримку шляхом розробки спеціальних патчів для критично важливих програмних компонентів або скористатися послугами зовнішніх провайдерів, які надають постійну підтримку для визначених непідтримуваних компонентів на основі договірних стосунків. Такі договірні відносини можуть включати постачальників програмного забезпечення з відкритим кодом. Підвищений ризик використання непідтримуваних компонентів системи можна зменшити, наприклад, шляхом заборони підключення таких компонентів до публічних або неконтрольованих мереж або впровадження інших форм ізоляції.
16.3.	Зовнішні послуги для системи	Зовнішні послуги для системи надаються зовнішніми постачальниками послуг. Організації встановлюють відносини із зовнішніми постачальниками послуг у різний спосіб, зокрема через ділове партнерство, контракти, міжвідомчі угоди, домовленості про напрямки діяльності, ліцензійні угоди, спільні підприємства та обмін ланцюжками поставок. Відповідальність за управління ризиками, пов'язаними з використанням зовнішніх послуг для системи, залишається за організацією, відповідальною за захист службової інформації. Угоди про надання послуг визначають очікувані результати роботи, описують вимірювані результати та визначають засоби захисту, пом'якшення наслідків та вимоги до реагування на випадки невідповідності. Інформація від зовнішніх постачальників послуг щодо конкретних функцій, портів, протоколів і сервісів, які використовуються при наданні таких послуг, може бути корисною, коли необхідно визначити компроміси, пов'язані з обмеженням певних функцій і сервісів або блокуванням певних портів і протоколів. Ця вимога стосується 1.15.

№	Назва вимоги	Опис вимоги
17.	**Управління ризиками ланцюга постачання**	
17.1.	План управління ризиками ланцюга постачання	Залежність від продуктів, систем та послуг від зовнішніх постачальників і характер відносин з ними створюють підвищений рівень ризику для організації. Загрози, які можуть підвищити ризики безпеки, включають несанкціоноване виробництво, впровадження або використання підробок, фальсифікацію, крадіжки, впровадження шкідливого програмного забезпечення, вбудованого програмного забезпечення та обладнання, а також неналежні практики виробництва та розробки в ланцюгу постачання. Ризики ланцюга постачання можуть бути індивідуальними або в межах системи, компонента чи послуги. Управління ризиками ланцюга постачання є складним, багатогранним завданням, яке вимагає скоординованих зусиль усієї організації для побудови довірчих відносин і комунікації з внутрішніми та зовнішніми зацікавленими сторонами. Управління ризиками ланцюга постачання (SCRM) включає виявлення та оцінку ризиків, визначення відповідних заходів реагування на ризики, розробку планів SCRM для документування заходів реагування, а також моніторинг виконання планів. План SCRM на рівні системи є специфічним для впровадження і передбачає реалізацію політики, вимоги, обмеження та наслідки. Він може бути як окремим, так і включеним до планів безпеки системи. План SCRM охоплює управління, впровадження та моніторинг засобів контролю SCRM, а також розробку або підтримку систем протягом життєвого циклу розвитку системи для підтримки завдань і функцій організації. Оскільки ланцюги постачання можуть суттєво відрізнятися між організаціями та всередині них, плани SCRM розробляються з урахуванням індивідуальних програмних, організаційних та операційних потреб.
17.2.	Стратегії придбання, інструменти і методи	Процес придбання є важливим засобом захисту ланцюга постачання. Існує багато корисних інструментів і методів, зокрема, приховування кінцевого використання системи або компонента системи, використання нецільових придбань, використання упаковки, що унеможливлює несанкціоноване втручання, або використання перевіреної чи контрольованої доставки. Результати оцінки ризиків у ланцюгу постачання можуть допомогти визначити стратегії, інструменти та методи, які найкраще підходять для конкретної ситуації. Інструменти та методи можуть забезпечити захист від несанкціонованого виробництва, крадіжок, фальсифікацій, підробок, впровадження шкідливого програмного забезпечення або "бекдорів", а також неналежних практик розробки протягом усього життєвого циклу системи.

№	Назва вимоги	Опис вимоги
		Організації також розглядають можливість створення стимулів для постачальників впроваджувати засоби контролю, сприяти прозорості їхніх процесів і практик безпеки, передбачати в контрактах заборону на використання зіпсованих або підроблених компонентів та обмежувати придбання у ненадійних постачальників. Організації розглядають можливість проведення тренінгів, освітніх та інформаційних програм для персоналу щодо ризиків у ланцюгу постачання, доступних стратегій їхнього зменшення, а також щодо того, коли ці програми слід застосовувати. Методи перевірки та захисту планів розвитку, документації та доказів повинні відповідати вимогам безпеки організації. У контрактах можуть бути визначені вимоги до захисту документації.
17.3.	Контроль ланцюга постачання і процесів	Елементи ланцюга постачання включають організації, суб'єкти або інструменти, які використовуються для дослідження, розробки, проектування, виробництва, придбання, доставки, інтеграції, експлуатації та обслуговування, а також виведення з експлуатації системи та компонентів системи. Процеси ланцюга постачання включають процеси розробки обладнання, програмного забезпечення, вбудованого програмного забезпечення та систем; процедури транспортування та обробки; програми кадрової та фізичної безпеки; інструменти управління конфігурацією, методи та заходи для збереження інформації про джерело походження; або інші програми, процеси чи процедури, пов'язані з розробкою, придбанням, обслуговуванням, виведення з експлуатації системи та компонентів системи. Елементи та процеси ланцюга постачання можуть надаватися організаціями, інтеграторами системи або зовнішніми постачальниками. Слабкі сторони або недоліки в елементах або процесах ланцюга постачання є потенційними вразливими місцями, які можуть бути використані зловмисниками, щоб завдати шкоди організації та вплинути на її здатність виконувати свої основні завдання або функції.