ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
___ _____ 2024 року № _____

РЕКОМЕНДАЦІЇ
з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації

І. Загальні положення

1. Ці Рекомендації описують порядок дій щодо проведення оцінки реалізації базового та цільового профілів безпеки на базі яких створювалась комплексна система захисту інформації у визначеній інформаційній, електронній комунікаційній та інформаційно-комунікаційній системі (далі – система).

2. Ці Рекомендації можуть використовуватися при проведенні внутрішньої та/або зовнішньої оцінки достатності заходів захисту інформації комплексних систем захисту інформації в системах, створених з використанням профілів безпеки.

3. Ці Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер та не встановлюють правових норм і є добровільними для використання.

4. Ці Рекомендації розроблено відповідно до підпункту 7 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, постанови Кабінету Міністрів України від 30 травня 2024 року № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, побудованих з використанням профілів безпеки інформації».

5. Ці Рекомендації розроблено з урахуванням вимог міжнародних стандартів NIST SP 800-53a Rev. 5 «Assessing Security and Privacy Controls in Information Systems and Organizations» та NIST SP 800-171a Rev.3 «Assessing Security Requirements for Controlled Unclassified Information».

6. У цих Рекомендаціях терміни вживаються у значенні, наведеному в Законах України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації» «Про Державну службу спеціального зв'язку та захисту інформації України», постанові Кабінету Міністрів України від 30 травня 2024 року № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, побудованих з використанням профілів безпеки інформації» та інших нормативних документах сфери захисту інформації.

7. Оцінка достатності заходів захисту інформації комплексних систем захисту інформації включає:

оцінку визначення цільового профілю безпеки;

оцінку реалізації базового профілю безпеки;

оцінку реалізації цільового профілю безпеки.

II. Оцінка визначення цільового профілю безпеки

1. Оцінка визначення цільового профілю безпеки проводиться з метою:

підтвердження відповідності вибору базового профілю безпеки для формування цільового профілю безпеки;

підтвердження наявності у цільовому профілі безпеки всіх вимог та заходів захисту базового профілю безпеки;

підтвердження відповідності цільового профілю безпеки (сукупності заходів із захисту інформації та їх налаштувань) вимогам законодавства та стандартів у сфері захисту інформації, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки тощо для визначеної системи.

2. Оцінка визначення цільового профілю безпеки здійснюється власником системи.

3. Позитивна оцінка визначення цільового профілю безпеки може бути підставою для його затвердження.

III. Оцінка реалізації базового профілю безпеки

1. Оцінка реалізації базового профілю безпеки здійснюється з метою підтвердження відповідності комплексної системи захисту інформації вимогам базового профілю безпеки.

2. Процедура оцінки базового профілю безпеки складається з мети заходу з оцінки та набору потенційних методів і об'єктів оцінки, які можуть бути використані для проведення оцінки. Кожна потенційна мета заходу з оцінки передбачає твердження про визначення, пов'язане з вимогою безпеки визначеною базовим профілем. Якщо у вимозі з безпеки є параметр, визначений організацією (ODP), то мета заходу з оцінки починається з формулювання, пов'язаного з визначенням ODP. Визначальні твердження пов'язані зі змістом вимог з безпеки, щоб допомогти забезпечити простежуваність результатів оцінки до вимог. Об'єкти оцінки визначають конкретні елементи, що оцінюються, і можуть містити специфікації, механізми, види діяльності та осіб. Специфікації – задокументовані об'єкти (наприклад, плани, політики, процедури, вимоги, функціональні специфікації та специфікації забезпечення, архітектури та проєктна документація), пов'язані із системою. Механізми – апаратні, програмні та мікропрограмні засоби захисту, реалізовані в системі. Дії – пов'язані із захистом дії, що підтримують систему, які передбачають залучення людей (наприклад, проведення операцій резервного копіювання системи, виконання плану реагування на інциденти та моніторинг мережевого трафіка). Особи – люди, які застосовують специфікації, механізми або заходи, описані вище.

3. Методи оцінки визначають характер і обсяг дій оцінювача і використовуються для полегшення розуміння, досягнення роз'яснень або отримання доказів. Потенційні методи оцінки передбачають дослідження, опитування та випробування:

метод дослідження – процес огляду, вивчення, інспектування, спостереження або аналізу об'єктів оцінки;

метод опитування – процес проведення дискусій з окремими особами або групами щодо об'єктів оцінки;

метод випробування – процес виконання об'єктами оцінки (тобто діями, механізмами) певних дій у визначених умовах з метою порівняння фактичної поведінки з очікуваною.

Методи оцінки містять атрибути глибини та охоплення, які визначають ретельність, обсяг і рівень зусиль для проведення оцінки, а також ступінь впевненості в тому, що вимоги з безпеки були виконані.

Потенційні об’єкти та методи оцінки наведено у таблиці 1.

Таблиця 1

Метод оцінки	Об’єкти	Опис
Дослідження	Політики та процедури, проєктна та супутня документація, налаштування конфігурацій, журнали аудиту тощо	Оцінювач ознайомлюється та вивчає об’єкт та приймає вмотивоване рішення щодо коректності реалізації відповідної вимоги з безпеки. Рішення відображається у звіті оцінювача
Опитування	Відповідальні посадові особи та уповноважений персонал	Оцінювач може проводити співбесіди із залученими працівниками для кращого розуміння реалій впровадження вимоги з безпеки. Рішення за результатами співбесіди вказується у звіті оцінювача
Випробування	Автоматизовані механізми	Оцінювач проводить тестові випробування автоматизованих механізмів, розгорнутих для забезпечення реалізації вимоги з безпеки. Результати тестування вказуються у звіті оцінювача

4. Структура та зміст типової процедури оцінки наведені нижче.

У таблиці 2 наведено приклад звіту з оцінки вимоги з безпеки «Невдалі спроби входу в систему» базового профілю.

Рекомендації з оцінки реалізації базового профілю безпеки який визначено наказом Адміністрації Держспецзв’язку від 24.06.2024 № 317 «Про визначення Базового профілю безпеки інформації» для систем де обробляється відповідна інформація за видом доступу наведені у додатках 1, 2 до цих Рекомендацій.

Таблиця 2

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
1.8	Невдалі спроби входу в систему			
	A.1.8.ODP[01]	визначена кількість послідовних невдалих спроб входу користувача в систему, дозволених протягом певного періоду часу;	П	*Дослідження:* 1. В політиці безпеки організації, яка затверджена наказом директора №111 від 26.06.2024 року, у розділі «Політика використання паролів» визначено кількість послідовних недійсних спроб входу до системи – 5 спроб; 3. В документі «Технічний проект. Пояснювальна записка» (реєстр. № 123 від 26.06.2024 року) у відповідності до пункту 4 розділу 3 політика використання паролів реалізується засобами ОС Windows 10 (параметр

				налаштування «Account lockout threshold»). 3. В налаштуваннях ОС Windows 10 системи параметр «Account lockout threshold» встановлено «5». *Опитування:* 1. Адміністратор безпеки - здійснив налаштування системи у відповідності до «Інструкції адміністратора безпеки» (реєстр. № 121 від 26.06.2024 року) та документу «Технічний проект. Пояснювальна записка» (реєстр. № 123 від 26.06.2024 року). *Випробування:* 1. Після 5 спроб введення неправильного паролю до ОС Windows 10 система блокується.
	A.1.8.ODP[02]	визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача;	Н	*Дослідження:* 1. В політиці безпеки організації, яка затверджена наказом директора №111 від 26.06.2024 року, у розділі «Політика використання паролів» визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача – 5 хвилин. 2. Механізми реалізації вимоги **не визначені.** 3. Спосіб налаштування механізмів **не визначено.** *Опитування:* 1. Адміністратор безпеки - відповідні налаштування системи **не проводив**. *Випробування:* 1. В продовж 7 хвилин здійснено 4 спроби введення неправильного паролю до ОС Windows 10 системи - система **не блокується.**
	A.1.8	визначено кількість послідовних невірних спроб входу користувача протягом <A.1.8.ODP[02]: період часу> обмежено до	Н	*Коментарі:* 1. Вимога не може бути оцінена - A.1.8.ODP[02] **оцінена негативно**.

		<A.1.8.ODP[01]: кількість>.		
	Загальна оцінка реалізації вимоги 1.8		**Не реалізовано**	

Номер вимоги у графі «№ вимоги» таблиці 2 відповідає номеру вимоги з безпеки базового профілю для систем де обробляється відповідна інформації за видом доступу.

Позначення заходів з оцінки мають буквено-цифрові ідентифікатори. Кожний захід з оцінки починається з літери «А», яка вказує на те, що воно є частиною процедури оцінки. Наступна послідовність цифр та/або літер (наприклад, 1.8.ODP[01]) вказує на ідентифікатор вимоги безпеки з базового профілю для ІКС де обробляється відповідна інформації за видом доступу (та конкретний елемент контролю, якщо це багатокомпонентна вимога), яка є метою заходу з оцінки. Параметри, визначені організацією, позначаються літерами «ODP». Якщо в заяві про визначення є декілька ODP, номер ODP вказується в квадратних дужках (наприклад, A.1.8.ODP[01]). Квадратні дужки також використовуються для позначення того, коли процедура оцінки далі розбиває вимогу на більш детальні заяви про визначення (наприклад, A.1.8.ODP[01], A.1.8.ODP[02]).

5. Застосування процедури оцінки до вимоги з безпеки дає результати оцінки або висновки. Висновки узагальнюються і використовуються як докази для визначення того, чи була вимога безпеки виконана або не виконана. Висновок «позитивний» вказує на те, що мета оцінки була досягнута і отримано повністю прийнятний результат. Висновок «негативний» означає, що існують потенційні аномалії, на які організація повинна звернути увагу. Висновок «не реалізовано» може також означати, що експерт не зміг отримати достатньої інформації для прийняття рішення, яке вимагається у звіті про результати оцінки.

Кожний висновок про оцінку, що виконана експертом, містить один з таких висновків: позитивно (П) або негативно (Н). Висновок «позитивний» вказує на те, що мета заходу з оцінки була досягнута і отримано повністю прийнятний результат. Висновок «негативний» означає, що існують потенційні аномалії, на які організація повинна звернути увагу. Висновок «негативний» може також означати, що експерт не зміг отримати достатньої інформації для прийняття рішення, яке вимагається у звіті про результати оцінки.

За результатами висновків з оцінки, визначається загальна оцінка реалізації вимоги з безпеки: «реалізовано» або «не реалізовано». Для отримання оцінки «реалізовано» всі висновки з оцінки визначеної вимоги з безпеки повинні дорівнювати «позитивно».

Висновок щодо позитивного результату оцінки реалізації базового профілю робиться у випадку отримання позитивного результату оцінки кожного заходу захисту кожної вимоги з безпеки.

IV. Оцінка реалізації цільового профілю безпеки

1. Оцінка реалізації цільового профілю безпеки здійснюється з метою підтвердження відповідності комплексної системи захисту інформації вимогам цільового профілю безпеки.

2. Оцінка реалізації заходів захисту цільового профілю безпеки здійснюється у відповідності до НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

3. Процедури, методи оцінки та форму звіту з оцінки можливо використовувати ті, що наведені у розділі ІІІ цих Рекомендацій.

4. Висновок щодо позитивного результату оцінки реалізації цільового профілю безпеки робиться у випадку отримання позитивного результату оцінки кожного заходу захисту, який входить до цього цільового профілю безпеки.

5. При проведені оцінки реалізації цільового профілю безпеки можливо враховувати результати отримані при оцінці реалізації базового профілю безпеки.

6. Позитивна оцінка реалізації базового та цільового профілю безпеки є підставою для декларування відповідності комплексної системи захисту інформації системи.

V. Оцінка засобів захисту інформації зі складу комплексної системи захисту інформації

1. У разі використання засобів технічного захисту інформації, які не мають підтвердження відповідності на момент проектування системи, відповідна оцінка проводиться під час оцінки реалізації базового та цільового профілів безпеки.

2. Власник (розпорядник) системи або проектувальник системи під час реалізації вимог з безпеки, визначених цільовим профілем безпеки інформації, обґрунтовує вибір зазначених засобів:

визначає механізми із захисту інформації, які повинні бути реалізовані засобом у системі;

отримує докази щодо реалізації механізмів із захисту інформації в засобі шляхом аналізу документації розробника засобу, проведенням відповідного налаштування та тестування засобу.

3. Для проведення зазначених робіт рекомендовано використовувати:

НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»;

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;

НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;

НД ТЗІ 2.7-009-09. «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»;

НД ТЗІ 2.7-010-09. «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»;

Можливості розповсюдження та/або перетину окремих складників критеріїв, наведених у НД ТЗІ 2.5-004-99, та заходів захисту, що визначені НД ТЗІ 3.6-006-24, наведено у додатку Г до НД ТЗІ 3.6-006-24.

4. Під час оцінки реалізації базового та цільового профілів безпеки проводиться оцінка обґрунтування вибору та застосування засобів технічного захисту інформації, які не мають підтвердження відповідності. Результати оцінки зазначаються у звіті з оцінки окремим розділом.

5. Засоби криптографічного захисту інформації, які входять до складу комплексної системи захисту інформації, повинні мати документи про оцінку відповідності.

Директор
ДЗІ Адміністрації Держспецзв'язку
лейтенант Олександр ГРИЩЕНКО

Додаток 1
до Рекомендацій з оцінки достатності
заходів захисту інформації
комплексних систем захисту
інформації в інформаційних,
електронних комунікаційних та
інформаційно-комунікаційних
системах, створених з використанням
профілів безпеки інформації
(пункт 4 розділу III)

Рекомендації
з оцінки реалізації базового профілю безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, де обробляється відкрита інформація

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
1.1	Управління обліковими записами			
	A.1.1.1[01]	визначено дозволені типи облікових записів у системі;		
	A.1.1.1[02]	визначено заборонені типи облікових записів у системі;		
	A.1.1.2[01]	облікові записи створюються відповідно до політики організації, процедур, умов та критеріїв організації;		
	A.1.1.2[02]	облікові записи увімкнуто відповідно до політики організації, процедур, умов та критеріїв організації;		
	A.1.1.2[03]	облікові записи модифікуються відповідно до політики, процедур, умов та критеріїв організації;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.1.2[04]	облікові записи вимкнено відповідно до політики, процедур, умов та критеріїв організації;		
	A.1.1.2[05]	облікові записи в системі видаляються відповідно до політики, процедур, умов та критеріїв організації;		
	A.1.1.3[01]	визначено авторизованих користувачів системи;		
	A.1.1.3[02]	визначено приналежність до групи та ролі;		
	A.1.1.3[03]	визначено повноваження доступу (тобто привілеї);		
	A.1.1.4[01]:	доступ до системи дозволено на основі наявного дозволу на доступ;		
	A.1.1.4[02]:	доступ до системи дозволено на основі цільового використання системи;		
	A.1.1.5	проводиться моніторинг використання облікових записів у системі;		
	A.1.1.6[01]	співробітники або відповідні ролі організації отримують повідомлення про те, що облікові записи більше не потрібні;		
	A.1.1.6[02]	співробітники або ролі організації отримують повідомлення про звільнення;		
	A.1.1.6[03]	співробітники або ролі отримують сповіщення, коли використовується система або потрібно знати зміни для окремої особи.		
	Загальна оцінка реалізації вимоги 1.1			
1.2	Забезпечення доступу			
	A.1.2	застосовано затверджені повноваження для логічного доступу до відкритої та конфіденційної інформації та ресурсів у системі.		
	Загальна оцінка реалізації вимоги 1.2			
1.3	Управління інформаційними потоками			
	A.1.3	застосовано затверджені вимоги для управління потоками відкритої та конфіденційної інформації всередині системи та між підключеними системами.		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 1.3			
1.4	Розмежування обов’язків			
	A.1.4.1	визначено обов’язки осіб, які потребують розмежування;		
	A.1.4.2	встановлено правила авторизації доступу для підтримки розмежування обов’язків.		
	Загальна оцінка реалізації вимоги 1.4			
1.5	Мінімізація повноважень			
	A.1.5.ODP[01]	визначено функції безпеки для авторизованого доступу до системи;		
	A.1.5.ODP[02]	визначено важливу для безпеки інформацію для авторизованого доступу;		
	A.1.5.1	доступ користувачів (або процесів, що діють від імені користувачів) до системи дозволено лише тоді, коли це необхідно для виконання призначених завдань;		
	A.1.5.2[01]	дозволено доступ до <A.1.5.ODP[01] функцій безпеки>;		
	A.1.5.2[02]	дозволено доступ до <A.1.5.ODP[01] інформації, що стосується безпеки>.		
	Загальна оцінка реалізації вимоги 1.5			
1.6	Мінімізація повноважень – непривілейований доступ до незахищених функцій			
	A.1.6.ODP[01]	визначено персонал або ролі, до яких слід обмежити привілейовані облікові записи у системі;		
	A.1.6.1	привілейовані облікові записи у системі обмежено до <A.1.6.ODP[01]: персонал або ролі>;		
	A.1.6.2	користувачі (або ролі) з привілейованими обліковими записами зобов’язані використовувати непривілейовані облікові записи для доступу до незахищених функцій або інформації.		
	Загальна оцінка реалізації вимоги 1.6			
1.7	Мінімізація повноважень – Заборона непривілейованим користувачам виконувати привілейовані функції			
	A.1.7	непривілейованим користувачам заборонено виконувати привілейовані функції.		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 1.7			
1.8	Невдалі спроби входу в систему			
	A.1.8.ODP[01]	визначена кількість послідовних невдалих спроб входу користувача в систему, дозволених протягом певного періоду часу;		
	A.1.8.ODP[02]	визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача;		
	A.1.8	визначено кількість послідовних невірних спроб входу користувача протягом <1.8.ODP[02]: період часу> обмежено до <A.1.8.ODP[01]: кількість>.		
	Загальна оцінка реалізації вимоги 1.8			
1.9	Попередження про використання системи			
	A.1.9	відображається повідомлення в системі з попередженнями про конфіденційність і безпеку відповідно до застосованих правил керівних документів для відкритої та конфіденційної інформації перед тим, як надати доступ до системи.		
	Загальна оцінка реалізації вимоги 1.9			
1.10	Блокування пристрою			
	A.1.10.ODP[01]	вибрано одне або декілька з таких значень параметрів: {ініціювання блокування пристрою після <A.1.10.ODP[02] періоду неактивності; вимога до користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду};		
	A.1.10.ODP[02]	визначено період бездіяльності, після якого ініціюється блокування пристрою (якщо вибрано);		
	A.1.10.1	доступ до системи заборонено за <A.1.10.ODP[01]: вибране значення параметра(ів)>;		
	A.1.10.2	блокування пристрою зберігається доти, доки користувач не відновить доступ за		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		допомогою встановлених процедур ідентифікації та автентифікації;		
	A.1.10.3	інформація, яку раніше було видно на дисплеї, приховується за допомогою блокування пристрою із загальнодоступним зображенням.		
	Загальна оцінка реалізації вимоги 1.10			
1.11	Припинення сеансу			
	A.1.11.ODP[01]	визначено умови або події, які вимагають відключення сеансу;		
	A.1.11	сеанс користувача автоматично завершується після <A.1.11.ODP[01]: умови або тригерні події>.		
	Загальна оцінка реалізації вимоги 1.11			
1.12	Віддалений доступ			
	A.1.12.1[01]	визначено типи допустимого віддаленого доступу до системи;		
	A.1.12.1[02]	встановлено обмеження використання для кожного типу дозволеного віддаленого доступу до системи;		
	A.1.12.1[03]	визначено вимоги до конфігурації для кожного типу дозволеного віддаленого доступу до системи;		
	A.1.12.1[04]	для кожного типу дозволеного віддаленого доступу до системи встановлюються вимоги до підключення;		
	A.1.12.2	кожен тип віддаленого доступу до системи авторизується перед встановленням таких з’єднань;		
	A.1.12.3	віддалений доступ до системи маршрутизується через керовані точки контролю доступу;		
	A.1.12.4[01]	дозволено віддалене виконання привілейованих команд;		
	A.1.12.4[02]	дозволено віддалений доступ до інформації, важливої для безпеки.		
	Загальна оцінка реалізації вимоги 1.12			

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
1.13	Бездротовий доступ			
	A.1.13.1[01]	визначено кожен тип бездротового доступу до системи;		
	A.1.13.1[02]	для кожного типу бездротового доступу до системи визначено обмеження на використання;		
	A.1.13.1[03]	визначено вимоги до конфігурації для кожного типу бездротового доступу до системи;		
	A.1.13.1[04]	для кожного типу бездротового доступу до системи встановлюються вимоги до підключення;		
	A.1.13.2	кожен тип бездротового доступу до системи авторизується перед встановленням таких з'єднань.		
	Загальна оцінка реалізації вимоги 1.13			
1.14	Контроль доступу для мобільних пристроїв			
	A.1.14.1[01]	для мобільних пристроїв встановлено обмеження щодо використання;		
	A.1.14.1[02]	для мобільних пристроїв встановлено вимоги до конфігурації;		
	A.1.14.1[03]	для мобільних пристроїв встановлено вимоги до підключення;		
	A.1.14.2	дозволено підключення мобільних пристроїв до системи;		
	A.1.14.3	впроваджено повне шифрування носія інформації пристрою або шифрування на основі шифрування сховищ інформації (контейнерів) для захисту конфіденційності відкритої та конфіденційної інформації на мобільних пристроях.		
	Загальна оцінка реалізації вимоги 1.14			
1.15	Використання зовнішніх систем			
	A.1.15.ODP[01]	визначено умови, яким повинні відповідати зовнішні системи, перш ніж дозволити використання або доступ до цих систем авторизованим особам;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.15.ODP[02]	визначено вимоги щодо безпеки, які мають бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам;		
	A.1.15.1	використання зовнішніх систем, окрім систем, дозволених організацією;		
	A.1.15.2[01]	визначені такі умови, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам: <A.1.15.ODP[01]: умови та положення>;		
	A.1.15.2[02]	встановлюються такі вимоги безпеки, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованими особами: <A.1.15.ODP[02]: вимоги безпеки>;		
	A.1.15.3[01]	авторизованим особам дозволяється використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі відкритої та конфіденційної інформації тільки після перевірки виконання вимог безпеки в зовнішній системі, як зазначено в планах безпеки організації;		
	A.1.15.3[02]	авторизованим особам дозволяється використовувати зовнішню систему для доступу до організаційної системи або для обробки, зберігання чи передачі відкритої та конфіденційної інформації тільки після збереження затверджених угод про підключення або обробку даних з організацією, що розміщує зовнішню систему, з якою укладено відповідну угоду;		
	A.1.15.4	обмежено використання авторизованими особами портативних пристроїв зберігання даних, контрольованих організацією, у зовнішніх системах.		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 1.15			
1.16	Публічно доступний контент			
	A.1.16.1	авторизовані особи проходять навчання з метою нерозголошення відкритої та конфіденційної інформації в загальнодоступних системах;		
	A.1.16.2[01]	вміст публічно доступного контенту періодично перевіряється на наявність відкритої та конфіденційної інформації;		
	A.1.16.2[02]	видаляється відкрита та конфіденційна інформація з загальнодоступних систем у разі виявлення.		
	Загальна оцінка реалізації вимоги 1.16			
2.1	Навчання з підвищення обізнаності			
	A.2.1.ODP[01]	визначено події, які потребують навчання користувачів системи з питань безпеки;		
	A.2.1.1.1[01]	користувачам системи надається навчання з питань безпеки як частина початкового навчання для нових користувачів;		
	A.2.1.1.1[02]	навчання з питань безпеки надається користувачам системи періодично після початкового навчання;		
	A.2.1.1.2	навчання з питань безпеки проводиться для користувачів системи, коли цього вимагають зміни у системі або наступні <A.2.1.ODP[01] події>;		
	A.2.1.2[01]	зміст тренінгу з безпекової обізнаності періодично оновлюється;		
	A.2.1.2[02]	зміст тренінгу з безпекової обізнаності оновлено після <A.2.1.ODP[01] подій>.		
	Загальна оцінка реалізації вимоги 2.1			
2.2	Рольове навчання			
	A.2.2.ODP[01]	визначено події, яких потребують тренінги з безпеки, для персоналу організації на основі покладених обов’язків;		
	A.2.2.1.1[01]	персонал організації проходить тренінги з безпеки на основі покладених обов’язків		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		перед наданням доступу до системи або відкритої та конфіденційної інформації;		
	A.2.2.1.1[02]	персонал організації проходить тренінги з безпеки на основі покладених обов’язків перед виконанням призначених обов'язків;		
	A.2.2.1.1[03]	тренінги з безпеки на основі покладених обов’язків проводяться для персоналу організації періодично після першого доступу;		
	A.2.2.1.2	тренінги з безпеки на основі покладених обов’язків проводяться для персоналу організації, коли цього вимагають зміни в системі або після <A.2.2.ODP[01] події>;		
	A.2.2.2[01]	зміст тренінгів з безпеки на основі покладених обов’язків періодично оновлюється;		
	A.2.2.2[02]	зміст тренінгів з безпеки на основі покладених обов’язків оновлено після <A.2.2.ODP[01] подій>.		
	Загальна оцінка реалізації вимоги 2.2			
3.1	Події аудиту			
	A.3.1.ODP[01]	визначено типи подій, вибраних для реєстрації у системі;		
	A.3.1.1	визначено такі типи подій для реєстрації у системі: <A.3.1.ODP[01] типи подій>;		
	A.3.1.2[01]	періодично переглядаються типи подій, вибрані для реєстрації;		
	A.3.1.2[02]	періодично оновлюються типи подій, вибрані для реєстрації.		
	Загальна оцінка реалізації вимоги 3.1			
3.2	Зміст записів аудиту			
	A.3.2.1[01]:	записи аудиту містять інформацію, яка дозволяє встановити, який тип події стався;		
	A.3.2.1[02]:	записи аудиту містять інформацію, яка дозволяє встановити, коли відбулася подія;		
	A.3.2.1[03]:	записи аудиту містять інформацію, яка встановлює, де відбулася подія;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.3.2.1[04]:	записи аудиту містять інформацію, яка встановлює джерело події;		
	A.3.2.1[05]:	записи аудиту містять інформацію, яка встановлює результат події;		
	A.3.2.1.[06]:	записи аудиту містять інформацію, що встановлює особу, суб'єкта, об'єкта або організацію, пов'язану з подією;		
	A.3.2.2:	додаткова інформація для записів аудиту надається у разі потреби.		
	Загальна оцінка реалізації вимоги 3.2			
3.3	Збереження записів аудиту			
	A.3.3.1	згенеровано записи аудиту для вибраних типів подій і згідно з вмістом записів аудиту, вказаних в 3.1 та в 3.2;		
	A.3.3.2	записи аудиту зберігаються протягом періоду часу, який відповідає політиці зберігання записів аудиту.		
	Загальна оцінка реалізації вимоги 3.3			
3.4	Реагування на відмови обробки даних аудиту			
	A.3.4.ODP[01]	визначено період часу, протягом якого персонал організації або ролі отримують сповіщення у разі відмови обробки даних аудиту;		
	A.3.4.ODP[02]	визначено додаткові дії, які слід виконати у разі відмови обробки даних аудиту;		
	A.3.4.1	персонал або ролі організації отримують сповіщення у разі відмови в процесі обробки даних аудиту в межах <A.3.4.ODP[01] періоду часу>;		
	A.3.4.2	наступні додаткові дії виконуються у разі відмови в процесі реєстрації аудиту: <A.3.4.ODP[02] додаткові дії>.		
	Загальна оцінка реалізації вимоги 3.4			
3.5	Огляд, аналіз і звітність аудиту			
	A.3.5.1	записи аудиту системи періодично переглядаються та аналізуються на предмет		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		виявлення ознак та потенційного впливу не властивої або незвичної діяльності;		
	A.3.5.2	результати аудиту доводяться до відома співробітникам організації або ролям;		
	A.3.5.3	записи аудиту в різних сховищах аналізуються та зіставляються задля забезпечення ситуативної обізнаності в масштабах організації.		
	Загальна оцінка реалізації вимоги 3.5			
3.6	Скорочення записів аудиту та формування звіту			
	A.3.6.1	впроваджено функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, вимоги до звітності та постфактум розслідування інцидентів;		
	A.3.6.2	збережено оригінальний зміст і часовий порядок записів аудиту.		
	Загальна оцінка реалізації вимоги 3.6			
3.7	Позначка часу			
	A.3.7.ODP[01]	визначено деталізацію вимірювання часу для позначок часу записів аудиту;		
	A.3.7.1	використовується внутрішній годинник у системі для генерування позначок часу записів аудиту;		
	A.3.7.2[01]	відповідають позначки часу для записів аудиту <A.3.7.ODP[01] деталізація вимірювання часу>;		
	A.3.7.2[02]	позначки часу для записів аудиту використовують всесвітній координований час (UTC), мають фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу як частину позначки часу.		
	Загальна оцінка реалізації вимоги 3.7			
3.8	Захист інформації аудиту			
	A.3.8.1	інформація аудиту та інструменти журналювання аудиту захищені від		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		несанкціонованого доступу, модифікації та видалення;		
	A.3.8.2	доступ до управління функціями аудиту дозволено лише підмножині привілейованих користувачів або ролей.		
	Загальна оцінка реалізації вимоги 3.8			
4.1	Базова конфігурація			
	A.4.1.1[01]	розроблено поточну базову конфігурацію системи;		
	A.4.1.1[02]	підтримується поточна базова конфігурація системи під контролем конфігурації;		
	A.4.1.2[01]	періодично переглядається базова конфігурація системи;		
	A.4.1.2[02]	переглядається базова конфігурація системи при встановленні або модифікації компонентів системи;		
	A.4.1.2[03]	періодично оновлюється базова конфігурація системи;		
	A.4.1.2[04]	оновлюється базова конфігурація системи, коли встановлюються або змінюються компоненти системи.		
	Загальна оцінка реалізації вимоги 4.1			
4.2	Налаштування конфігурації			
	A.4.2.ODP[01]	визначено параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам;		
	A.4.2.1[01]	визначено та задокументовано такі параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: <A.4.2.ODP[01] налаштування конфігурації>;		
	A.4.2.1[02]	реалізовано такі налаштування конфігурації системи: <A.4.2.ODP[01] налаштування конфігурації>;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.2.2[01]	визначено та задокументовано будь-які відхилення від встановлених параметрів конфігурації;		
	A.4.2.2[02]	затверджено всі відхилення від встановлених налаштувань конфігурації.		
	Загальна оцінка реалізації вимоги 4.2			
4.3	Управління змінами конфігурації			
	A.4.3.1	визначено типи змін у конфігурації системи, які необхідно контролювати;		
	A.4.3.2[01]	переглядаються запропоновані зміни в конфігурації системи, які необхідно контролювати;		
	A.4.3.2[02]	запропоновані зміни в конфігурації системи схвалюються або відхиляються з урахуванням впливу на безпеку;		
	A.4.3.3[01]	впроваджуються затверджені зміни в конфігурації системи, які необхідно контролювати;		
	A.4.3.3[02]	задокументовані затверджені зміни в конфігурації системи, які необхідно контролювати;		
	A.4.3.4[01]	відстежуються дії, пов'язані зі змінами конфігурації системи, які необхідно контролювати;		
	A.4.3.4[02]	переглядаються дії, пов'язані зі змінами конфігурації системи, які необхідно контролювати.		
	Загальна оцінка реалізації вимоги 4.3			
4.4	Аналіз впливу на безпеку та приватність			
	A.4.4	проводиться аналіз впливу змін у системі на безпеку перед їх впровадженням.		
	Загальна оцінка реалізації вимоги 4.4			
4.5	Обмеження доступу до змін			
	A.4.5[01]	визначено та задокументовано фізичні та логічні обмеження доступу, пов'язані зі змінами в системі;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.5[02]	затверджені обмеження фізичного доступу, пов'язані зі змінами в системі;		
	A.4.5[03]	застосовуються обмеження фізичного доступу, пов'язані зі змінами в системі;		
	A.4.5[04]	визначені та задокументовані логічні обмеження доступу, пов'язані зі змінами в системі;		
	A.4.5[05]	затверджені логічні обмеження доступу, пов'язані зі змінами в системі;		
	A.4.5[06]	введено в дію логічні обмеження доступу, пов'язані зі змінами в системі.		
	Загальна оцінка реалізації вимоги 4.5			
4.6	Мінімально необхідна функціональність			
	A.4.6.ODP[01]	визначено функції, які потрібно заборонити або обмежити;		
	A.4.6.ODP[02]	визначено порти, які потрібно заборонити або обмежити;		
	A.4.6.ODP[03]	визначено протоколи, які потрібно заборонити або обмежити;		
	A.4.6.ODP[04]	визначено з'єднання, які потрібно заборонити або обмежити;		
	A.4.6.ODP[05]	визначено служби, які потрібно заборонити або обмежити;		
	A.4.6.ODP[06]	визначено функції, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[07]	визначено порти, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[08]	визначено протоколи, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[09]	визначено з'єднання, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[10]	визначено служби, які вважаються непотрібними або небезпечними;		
	A.4.6.1	система налаштована на надання лише необхідних для виконання завдань і функцій;		
	A.4.6.2[01]	заборонено або обмежено використання таких функцій: <A.4.6.ODP[01]: функції>;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.6.2[02]	заборонено або обмежено використання таких портів: <A.4.6.ODP[02]: порти>;		
	A.4.6.2[03]	використання таких протоколів заборонено або обмежено: <A.4.6.ODP[03]: протоколи>;		
	A.4.6.2[04]	заборонено або обмежено використання таких з'єднань: <A.4.6.ODP[04]: з’єднання>;		
	A.4.6.2[05]	заборонено або обмежено використання таких служб: <A.4.6.ODP[05]: служби>;		
	A.4.6.3	система періодично переглядається для виявлення непотрібних або небезпечних функцій, портів, протоколів, з'єднань і служб;		
	A.4.6.4[01]	вимкнено або видалено такі непотрібні або небезпечні функції: <A.4.6.ODP[06]: функції>;		
	A.4.6.4[02]	вимкнено або вилучено такі непотрібні або небезпечні порти: <A.4.6.ODP[07]: порти>;		
	A.4.6.4[03]	вимкнено або вилучено такі непотрібні або небезпечні протоколи: <A.4.6.ODP[08]: протоколи>;		
	A.4.6.4[04]	вимкнено або видалено такі непотрібні або небезпечні з'єднання: <A.4.6.ODP[09]: з’єднання>;		
	A.4.6.4[05]	вимкнено або вилучено такі непотрібні або небезпечні служби: <A.4.6.ODP[10]: служби>.		
	Загальна оцінка реалізації вимоги 4.6			
5.1	Ідентифікація та автентифікація (користувачів організації)			
	A.5.1[01]	користувачі системи унікально ідентифіковані та автентифіковані;		
	A.5.1[02]	унікальна ідентифікація автентифікованих користувачів системи пов'язана з процесами, що діють від імені цих користувачів.		
	Загальна оцінка реалізації вимоги 5.1			
5.2	Ідентифікація та автентифікація пристроїв			
	A.5.2	пристрої унікально ідентифікуються та автентифікуються перед встановленням з'єднання із системою.		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 5.2			
5.3	Ідентифікація та автентифікація (користувачів організації) – багатофакторна автентифікація привілейованих облікових записів			
	A.5.3	реалізовано багатофакторну автентифікацію для доступу до облікових записів системи.		
	Загальна оцінка реалізації вимоги 5.3			
5.4	Ідентифікація та автентифікація (користувачів організації) – доступ до облікових записів – стійкість до відтворення			
	A.5.4	реалізовано стійкі до повторного відтворення механізми автентифікації для доступу до облікових записів у системі.		
	Загальна оцінка реалізації вимоги 5.4			
5.5	Управління ідентифікацією			
	A.5.5.ODP[01]	визначено персонал або ролі, від яких необхідно отримати дозвіл на призначення ідентифікатора;		
	A.5.5.ODP[02]	визначено період часу для запобігання повторному використанню ідентифікаторів;		
	A.5.5.1	отримано дозвіл від <A.5.5.ODP[01]: персонал або ролі> на призначення ідентифікатора особи, групи, ролі, служби або пристрою;		
	A.5.5.2[01]	вибрано ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій;		
	A.5.5.2[02]	призначено ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій;		
	A.5.5.3	запобігання повторному використанню ідентифікаторів для <A.5.5.ODP[02]: період часу>.		
	Загальна оцінка реалізації вимоги 5.5			
5.6	Управління автентифікатором – автентифікація на основі пароля			
	A.5.6.ODP[01]	правила складу та складності паролів;		
	A.5.6.1[01]	ведеться список часто використовуваних, очікуваних або скомпрометованих паролів;		
	A.5.6.1[02]	періодично оновлюється список часто використовуваних, очікуваних або скомпрометованих паролів;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.5.6.1[03]	оновлюється список часто використовуваних, очікуваних або скомпрометованих паролів у разі виникнення підозри, що паролі організації були скомпрометовані;		
	A.5.6.2	перевіряються паролі на відсутність у списку часто використовуваних, очікуваних або скомпрометованих паролів, коли вони створюються або оновлюються користувачами;		
	A.5.6.3	передаються паролі лише криптографічно захищеними каналами;		
	A.5.6.4	зберігаються паролі у криптографічно захищеному вигляді;		
	A.5.6.5	буде обрано новий пароль під час першого використання після відновлення облікового запису;		
	A.5.6.6	виконуються такі правила складу та складності: <A.5.6.ODP[01]: правила>.		
	Загальна оцінка реалізації вимоги 5.6			
5.7	Зворотний зв'язок автентифікатора			
	A.5.7.1	прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.		
	Загальна оцінка реалізації вимоги 5.7			
5.8	Управління автентифікатором			
	A.5.8.ODP[01]	визначені події, які викликають зміну або оновлення автентифікаторів;		
	A.5.8.1	перевірено ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора;		
	A.5.8.2	встановлено початковий вміст автентифікатора для всіх автентифікаторів, виданих організацією;		
	A.5.8.3[01]	створені та впроваджені адміністративні процедури для початкового розподілу автентифікаторів;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.5.8.3[02]	створені та впроваджені адміністративні процедури для втрачених, скомпрометованих або пошкоджених автентифікаторів;		
	A.5.8.3[03]	створені та впроваджені адміністративні процедури для відкликання автентифікаторів;		
	A.5.8.4	потрібно змінювати автентифікатори за замовчуванням при першому використанні;		
	A.5.8.5	потрібно періодично змінювати та оновлювати автентифікатори або коли відбуваються такі події: <A.5.8.ODP[01]: події >;		
	A.5.8.6[01]	захищено вміст автентифікатора від несанкціонованого розкриття;		
	A.5.8.6[02]	захищено вміст автентифікатора від несанкціонованої модифікації.		
	Загальна оцінка реалізації вимоги 5.8			
6.1	Обробка інциденту			
	A.6.1.1	розроблено план реагування на інциденти, який забезпечить організацію стратегією для реалізації її можливостей реагування на інциденти;		
	A.6.1.2[01]	впроваджено систему реагування на інциденти, яка відповідає плану реагування на інциденти;		
	A.6.1.2[02]	передбачено підготовку до реагування на інциденти;		
	A.6.1.2[03]	передбачає систему реагування на інциденти, виявлення та аналіз інцидентів;		
	A.6.1.2[04]	передбачає систему реагування на інциденти, локалізацію інцидентів;		
	A.6.1.2[05]	передбачає систему реагування на інциденти, ліквідацію наслідків інцидентів;		
	A.6.1.2[06]	передбачає систему реагування на інциденти, відновлення після інцидентів;		
	A.6.1.3	оновлюється план реагування на інциденти, щоб врахувати зміни в системі та зміни в організації або проблеми, що виникли під час		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		впровадження, виконання або тестування плану.		
	Загальна оцінка реалізації вимоги 6.1			
6.2	Моніторинг інциденту			
	A.6.2.ODP[01]	визначено період часу, протягом якого необхідно повідомляти про підозрілі інциденти до служби реагування на інциденти;		
	A.6.2.ODP[02]	визначені органи, яким слід повідомляти інформацію про інцидент;		
	A.6.2.1[01]	відстежуються інциденти, пов'язані з безпекою системи;		
	A.6.2.1[02]	документуються інциденти, пов'язані з безпекою системи;		
	A.6.2.2	повідомляється про підозрілі інциденти до служби реагування на інциденти в організації протягом <A.6.2.ODP[01]: період часу>;		
	A.6.2.3	надсилається інформація про інцидент до <A.6.2.ODP[02]: органів влади>;		
	A.6.2.4	надається підтримка реагування на інциденти, який пропонує поради та допомогу користувачам системи щодо обробки та звітування про інциденти.		
	Загальна оцінка реалізації вимоги 6.2			
6.3	Перевірка реагувань на інциденти			
	A.6.3	проводиться періодична перевірка ефективності системи реагування на інциденти.		
	Загальна оцінка реалізації вимоги 6.3			
6.4	Навчання з реагування на інциденти			
	A.6.4.ODP[01]	визначено період часу, протягом якого користувачі системи повинні пройти навчання з реагування на інциденти;		
	A.6.4.ODP[02]	визначені події, які ініціюють перегляд та оновлення змісту навчання з реагування на інциденти;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.6.4.1.[01]	проводиться навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків протягом <A.6.4.ODP[01]: період часу> після прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до системи;		
	A.6.4.1.[02]	навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків проводиться тоді, коли цього вимагають зміни в системі;		
	A.6.4.1.[03]	навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків проводиться періодично після початкового навчання та навчання, орієнтованого на конкретні події;		
	A.6.4.2[01]	проводиться періодичний перегляд змісту навчання з реагування на інциденти;		
	A.6.4.2[02]	переглядається зміст навчання з реагування на інциденти після <A.6.4.ODP[02]: події>;		
	A.6.4.2[03]	зміст навчання з реагування на інциденти періодично оновлюється;		
	A.6.4.2[04]	зміст навчання з реагування на інциденти оновлюється після <A.6.4.ODP[02]: події>.		
	Загальна оцінка реалізації вимоги 6.4			
7.1	Інструменти для обслуговування			
	A.7.1.1[01]	затверджується використання інструментів для обслуговування системи;		
	A.7.1.1[02]	контролюється використання інструментів для обслуговування системи;		
	A.7.1.2[03]	відстежується використання інструментів для обслуговування системи;		
	A.7.1.2	перевіряються інструменти для технічного обслуговування на предмет неналежних або несанкціонованих модифікацій;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.7.1.3	перевіряються носії, що містять діагностичні та тестові програми, на наявність шкідливого коду перед використанням у системі.		
	Загальна оцінка реалізації вимоги 7.1			
7.2	Віддалене обслуговування			
	A.7.2.1[01]	дозволені віддалені сеанси з технічного обслуговування та діагностики;		
	A.7.2.1[02]	проводиться моніторинг віддалених сеансів з технічного обслуговування та діагностики;		
	A.7.2.2	реалізована багатофакторна автентифікація та стійкість до повторного відтворення при створенні віддалених сеансів технічного обслуговування та діагностики;		
	A.7.2.3[01]	завершуються сеансові з'єднання після завершення віддаленого технічного обслуговування;		
	A.7.2.3[02]	розриваються мережеві з'єднання після завершення віддаленого технічного обслуговування.		
	Загальна оцінка реалізації вимоги 7.2			
7.3	Технічний персонал			
	A.7.3.1	запроваджено процес авторизації персоналу з технічного обслуговування;		
	A.7.3.2	ведеться список уповноважених організацій або персоналу з технічного обслуговування;		
	A.7.3.3	проводиться перевірка персоналу без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ;		
	A.7.3.4	призначається персонал організації з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю персоналу з технічного обслуговування, який не має необхідних повноважень доступу.		
	Загальна оцінка реалізації вимоги 7.3			
8.1	Зберігання носіїв інформації			

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.8.1[01]	здійснюється фізичний контроль носіїв інформації, що містять відкриту та конфіденційну інформацію, до моменту їх знищення або очищення за допомогою затвердженого обладнання, методів і процедур;		
	A.8.1[02]	надійно зберігаються носії інформації, що містять відкриту та конфіденційну інформацію, до моменту їх знищення або очищення за допомогою затвердженого обладнання, методів і процедур.		
	Загальна оцінка реалізації вимоги 8.1			
8.2	Доступ до носіїв інформації			
	A.8.2	обмежено доступ до відкритої та конфіденційної інформації на носіях інформації.		
	Загальна оцінка реалізації вимоги 8.2			
8.3	Знищення інформації на носіях інформації			
	A.8.3	проходять очищення носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією, виходом з-під контролю організації або перед повторним використанням.		
	Загальна оцінка реалізації вимоги 8.3			
8.4	Маркування носіїв інформації			
	A.8.4[01]	на носіях інформації, що містять відкриту та конфіденційну інформацію, наявне маркування, що вказує на обмеження розповсюдження;		
	A.8.4[02]	на носіях інформації, що містять відкриту та конфіденційну інформацію, наявне маркування щодо застережень поводження з ними;		
	A.8.4[03]	на носіях інформації, що містять відкриту та конфіденційну інформацію, наявне маркування щодо позначок безпеки.		
	Загальна оцінка реалізації вимоги 8.4			

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
8.5	Транспортування носіїв інформації			
	A.8.5.1[01]	носії інформації, що містять відкриту та конфіденційну інформацію, захищені під час транспортування за межі контрольованих територій;		
	A.8.5.1[02]	носії інформації, що містять відкриту та конфіденційну інформацію, контролюються під час транспортування за межі контрольованих територій;		
	A.8.5.2	зберігається облік носіїв інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій;		
	A.8.5.3	застосовуються криптографічні механізми для запобігання несанкціонованому доступу до відкритої та конфіденційної інформації, що зберігається на носіях інформації, під час транспортування.		
	Загальна оцінка реалізації вимоги 8.5			
8.6	Використання носіїв інформації			
	A.8.6.ODP[01]	визначено типи носіїв інформації, використання яких обмежено або заборонено;		
	A.8.6.1	обмежено або заборонено використання таких типів носіїв інформації: <A.8.6.ODP[01]: типи носіїв інформації>;		
	A.8.6.2	заборонено використання знімних носіїв інформації без ідентифікованого власника.		
	Загальна оцінка реалізації вимоги 8.6			
9.1	Перевірка персоналу			
	A.9.1.ODP[01]	визначено умови, які вимагають повторної перевірки осіб;		
	A.9.1.1	особи проходять перевірку перед наданням доступу до системи;		
	A.9.1.2	особи проходять повторну перевірку відповідно до наведених нижче умов: <A.9.1.ODP[01]: умови>.		
	Загальна оцінка реалізації вимоги 9.1			

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
9.2	Звільнення персоналу. Переведення персоналу			
	A.9.2.ODP[01]	визначено період часу, протягом якого забороняється доступ до системи;		
	A.9.2.ODP[02]	визначено період часу, протягом якого мають бути виконані дії з переведення або призначення;		
	A.9.2.ODP[03]	визначені дії з переведення або призначення;		
	A.9.2.1[01]	після припинення індивідуальної трудової діяльності доступ до системи забороняється протягом <A.9.2.ODP[01]: період часу>;		
	A.9.2.1[02]	після припинення індивідуальної трудової діяльності припиняються або відкликаються пов'язані з нею автентифікатори та облікові дані;		
	A.9.2.1[03]	після припинення індивідуальної трудової діяльності відновлюються властивості системи, пов’язані із системою;		
	A.9.2.2[01]	при перепризначенні або переведенні працівників на інші посади в організації переглядаються та підтверджуються поточні оперативні потреби в поточних логічних та фізичних правах доступу до системи та об'єкта;		
	A.9.2.2[02]	при перепризначенні або переведенні працівників на інші посади в організації ініціюються <A.9.2.ODP[03]: дії з переведення або перепризначення> протягом <A.9.2.ODP[02]: період часу>;		
	A.9.2.2[03]	при перепризначенні або переведенні працівників на інші посади в організації повноваження доступу змінюються відповідно до будь-яких змін в оперативних потребах.		
	Загальна оцінка реалізації вимоги 9.2			
10.1	Авторизація фізичного доступу			

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.10.1.1[01]	розроблено список осіб, які мають право доступу до фізичного місця розташування системи;		
	A.10.1.1[02]	затверджено список осіб, які мають право доступу до фізичного місця розташування системи;		
	A.10.1.1[03]	підтримується список осіб, які мають право доступу до фізичного місця розташування системи;		
	A.10.1.2	надаються повноваження для доступу до об'єкта;		
	A.10.1.3	список фізичного доступу періодично перевіряється;		
	A.10.1.4	особи видаляються зі списку фізичного доступу, коли доступ більше не потрібен.		
	Загальна оцінка реалізації вимоги 10.1			
10.2	Моніторинг фізичного доступу			
	A.10.2.1[01]	проводиться моніторинг фізичного доступу до місця розташування системи для виявлення інцидентів фізичної безпеки;		
	A.10.2.1[02]	проводиться моніторинг фізичного доступу до місця розташування системи для реагування на інциденти фізичної безпеки;		
	A.10.2.2	журнали фізичного доступу періодично переглядаються.		
	Загальна оцінка реалізації вимоги 10.2			
10.3	Альтернативне робоче місце			
	A.10.3.ODP[01]	визначено вимоги безпеки, які необхідно дотримуватися на альтернативних робочих місцях;		
	A.10.3.1	визначені альтернативні робочі місця, дозволені для використання працівниками;		
	A.10.3.2	на альтернативних робочих місцях застосовуються такі вимоги безпеки: <A.10.3.ODP[01]: вимоги безпеки>.		
	Загальна оцінка реалізації вимоги 10.3			
10.4	Керування фізичним доступом			

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.10.4.ODP[01]	визначено обставини, що вимагають супроводу відвідувачів і контролю за їх діяльністю;		
	A.10.4.1[01]	фізичний доступ контролюється в місці розташування системи шляхом перевірки індивідуальних дозволів на фізичний доступ перед здійсненням доступу;		
	A.10.4.1[02]	фізичний доступ контролюється в місці розташування системи шляхом контролю входу та виходу за допомогою систем/пристроїв контролю фізичного доступу або охоронців;		
	A.10.4.2	ведуться журнали контролю фізичного доступу для точок входу та виходу;		
	A.10.4.3[01]	відвідувачі супроводжуються;		
	A.10.4.3[02]	діяльність відвідувачів контролюється за таких обставин: <A.10.4.ODP[01]: обставини>;		
	A.10.4.4[01]	забезпечений захист ключів;		
	A.10.4.4[02]	забезпечений захист кодів;		
	A.10.4.4[03]	забезпечений захист інших пристроїв фізичного доступу.		
	Загальна оцінка реалізації вимоги 10.4			
10.5	Контроль доступу до джерел і ліній електроживлення. Контроль доступу до пристроїв виведення інформації			
	A.10.5.1	контролюється фізичний доступ до розподільчих ліній системи та ліній електропередач на об'єктах організації;		
	A.10.5.2	фізичний доступ до пристроїв виведення контролюється, щоб запобігти доступу сторонніх осіб до відкритої та конфіденційної інформації.		
	Загальна оцінка реалізації вимоги 10.5			
11.1	Оцінювання ризику			
	A.11.1.1	оцінюється ризик несанкціонованого розголошення в результаті обробки,		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		зберігання або передачі конфіденційної інформації;		
	A.11.1.2	оцінювання ризиків періодично оновлюється.		
	Загальна оцінка реалізації вимоги 11.1			
11.2	Сканування вразливостей			
	A.11.2.ODP[01]	визначено час на реагування для усунення вразливостей системи;		
	A.11.2.1[01]	система періодично перевіряється на наявність вразливостей;		
	A.11.2.1[02]	система відстежується на наявність вразливостей, коли виявляються нові вразливості, що впливають на систему;		
	A.11.2.1[03]	система періодично сканується на наявність вразливостей;		
	A.11.2.1[04]	система сканується на вразливості при виявленні нових вразливостей, які впливають на систему;		
	A.11.2.2	усуваються вразливості системи протягом <A.11.2.ODP[01]: час на реагування>.		
	Загальна оцінка реалізації вимоги 11.2			
12.1	Оцінювання			
	A.12.1	вимоги до захисту інформації в системі та середовища її функціонування періодично оцінюються для визначення того, чи були виконані ці вимоги.		
	Загальна оцінка реалізації вимоги 12.1			
12.2	План усунення недоліків і контрольні показники			
	A.12.2.1[01]	розроблено план дій і контрольні показники з метою документування запланованих заходів з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки;		
	A.12.2.1[02]	розроблено план дій і контрольні показники з метою зменшення або усунення відомих недоліків системи;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.12.2.2[01]	існуючий план дій і контрольні показники періодично оновлюються на основі результатів оцінки безпеки;		
	A.12.2.2[02]	існуючий план дій і контрольні показники періодично оновлюються на основі результатів незалежних аудитів або оглядів;		
	A.12.2.2[03]	існуючий план дій і контрольні показники періодично оновлюються на основі результатів безперервного моніторингу.		
	Загальна оцінка реалізації вимоги 12.2			
12.3	Безперервний моніторинг			
	A.12.3[01]	розроблено та впроваджено стратегію безперервного моніторингу на рівні системи;		
	A.12.3[02]	постійний моніторинг внесений до стратегії безперервного моніторингу;		
	A.12.3[03]	оцінка безпеки внесена до стратегії безперервного моніторингу.		
	Загальна оцінка реалізації вимоги 12.3			
12.4	Взаємодія систем			
	A.12.4.ODP[01]	вибрано одне або декілька з наступних значень параметрів: {угоди про безпеку з'єднання; угоди про безпеку обміну інформацією; меморандуми або угоди про взаєморозуміння; угоди про рівень обслуговування; угоди з користувачами; угоди про нерозголошення інформації};		
	A.12.4.1	обмін відкритою та конфіденційною інформацією між системою та іншими системами затверджено та керується за допомогою <A.12.4.ODP[01]: вибране значення параметра(ів)>;		
	A.12.4.2[01]	характеристики інтерфейсу задокументовані як частина договорів про обмін;		
	A.12.4.2[02]	вимоги до безпеки задокументовані як частина договорів про обмін;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.12.4.2[03]	обов'язки для кожної системи задокументовані як частина договорів про обмін;		
	A.12.4.3[01]	договори про обмін періодично переглядаються;		
	A.12.4.3[02]	договори про обмін періодично оновлюються.		
	Загальна оцінка реалізації вимоги 12.4			
13.1	Захист периметра			
	A.13.1.1[01]	здійснюється контроль зв’язку на зовнішніх периметрах системи;		
	A.13.1.1[02]	здійснюється управління зв’язком на зовнішніх периметрах системи;		
	A.13.1.1[03]	здійснюється контроль зв’язку на ключових внутрішніх периметрах системи;		
	A.13.1.1[04]	здійснюється управління зв’язком на ключових внутрішніх периметрах системи;		
	A.13.1.2	підмережі реалізовані для загальнодоступних компонентів системи, які фізично або логічно відділені від внутрішніх мереж;		
	A.13.1.3	підключення до зовнішніх систем здійснюється лише через керовані інтерфейси, які складаються з пристроїв захисту периметра, розташованих відповідно до архітектури безпеки організації.		
	Загальна оцінка реалізації вимоги 13.1			
13.2	Інформація в загальних ресурсах системи			
	A.13.2[01]	запобігли несанкціонованій передачі інформації за допомогою загальних ресурсів системи;		
	A.13.2[02]	запобігли ненавмисній передачі інформації за допомогою загальних ресурсів системи.		
	Загальна оцінка реалізації вимоги 13.2			
13.3	Захист периметра - відмова за замовчуванням - дозвіл за винятком			
	A.13.3[01]	за замовчуванням заборонено трафік мережевих комунікацій;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.13.3[02]	трафік мережевих комунікацій дозволено за винятком.		
	Загальна оцінка реалізації вимоги 13.3			
13.4	Конфіденційність і цілісність передачі. Захист інформації в стані спокою			
	A.13.4[01]	реалізовано механізми криптографічного захисту для запобігання несанкціонованому розкриттю відкритої та конфіденційної інформації під час передачі;		
	A.13.4[02]	реалізовано механізми криптографічного захисту для запобігання несанкціонованому розкриттю відкритої та конфіденційної інформації під час зберігання.		
	Загальна оцінка реалізації вимоги 13.4			
13.5	Відключення мережі			
	A.13.5:	мережеві з'єднання, пов'язані із сеансами зв'язку, завершуються в кінці сеансів або після періодів бездіяльності.		
	Загальна оцінка реалізації вимоги 13.5			
13.6	Встановлення та управління криптографічними ключами			
	A.13.6.ODP[01]	визначено вимоги до встановлення та управління ключами;		
	A.13.6[01]	криптографічні ключі встановлюються в системі відповідно до таких вимог до управління ключами: <A.13.6.ODP[01]: вимоги>;		
	A.13.6[02]	управління криптографічними ключами в системі здійснюється відповідно до таких вимог до управління ключами: <A.13.6.ODP[01]: вимоги>.		
	Загальна оцінка реалізації вимоги 13.6			
13.7	Криптографічний захист			
	A.13.7.ODP:	визначено типи криптографії для захисту конфіденційності відкритої та конфіденційної інформації;		
	A.13.7:	для захисту конфіденційності відкритої та конфіденційної інформації при використанні		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		системи впроваджено такі типи криптографії: <A.13.7.ODP: типи криптографії>.		
	Загальна оцінка реалізації вимоги 13.7			
13.8	Спільні обчислювальні пристрої та застосунки			
	A.13.8.1	заборонено віддалено активувати спільні обчислювальні пристрої та програмне забезпечення;		
	A.13.8.2	чіткі вказівки щодо використання надаються користувачам, які фізично присутні біля пристроїв.		
	Загальна оцінка реалізації вимоги 13.8			
13.9	Мобільний код			
	A.13.9.1[01]	визначено прийнятний мобільний код;		
	A.13.9.1[02]	визначено прийнятні технології мобільного коду;		
	A.13.9.2[01]	використання мобільного коду авторизовано;		
	A.13.9.2[02]	відстежується використання мобільного коду;		
	A.13.9.2[03]	контролюється використання мобільного коду.		
	Загальна оцінка реалізації вимоги 13.9			
13.10	Автентифікація сесії			
	A.13.10	автентифікацію сеансів зв'язку захищено.		
	Загальна оцінка реалізації вимоги 13.10			
14.1	Виправлення дефектів			
	A.14.1.ODP[01]	визначено період часу, протягом якого слід встановити оновлення програмного забезпечення, що стосується безпеки, після випуску оновлення;		
	A.14.1.ODP[02]	визначено період часу, протягом якого слід встановити оновлення вбудованого програмного забезпечення, що стосується безпеки, після випуску оновлення;		
	A.14.1.1[01]	виявляються недоліки системи;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.14.1.1[02]	повідомляється про недоліки системи;		
	A.14.1.1[03]	виправляються недоліки системи;		
	A.14.1.2[01]	оновлення програмного забезпечення, що стосується безпеки, встановлюється протягом <A.14.1.ODP[01]: періоду часу> після випуску оновлення;		
	A.14.1.2[02]	оновлення вбудованого програмного забезпечення, що стосується безпеки, встановлюється протягом <A.14.1.ODP[02]: періоду часу> після випуску оновлення.		
	Загальна оцінка реалізації вимоги 14.1			
14.2	Захист від шкідливого коду			
	A.14.2.ODP[01]	визначено частоту, з якою механізми захисту від шкідливого коду виконують перевірку;		
	A.14.2.1[01]	у визначених місцях системи впроваджено механізми захисту для виявлення шкідливого коду;		
	A.14.2.1[02]	у визначених місцях системи впроваджено механізми захисту для знищення шкідливого коду;		
	A.14.2.2	механізми захисту від шкідливого коду оновлено з виходом нових версій відповідно до політики та процедур управління конфігурацією;		
	A.14.2.3.1[01]	механізми захисту від шкідливого коду налаштовано на виконання сканування системи <A.14.2.ODP[01]: частота>;		
	A.14.2.3.1[02]	механізми захисту від шкідливого коду налаштовано на виконання сканування файлів із зовнішніх джерел у режимі реального часу на кінцевих точках або точках входу та виходу з мережі під час завантаження, відкриття або виконання файлів;		
	A.14.2.3.2	механізми захисту від шкідливого коду налаштовано на блокування шкідливого коду,		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		поміщення шкідливого коду в карантин або виконання інших дій у відповідь на виявлення шкідливого коду.		
	Загальна оцінка реалізації вимоги 14.2			
14.3	Попередження, рекомендації та директиви з безпеки			
	A.14.3.1	попередження, рекомендації та директиви щодо безпеки системи від зовнішніх організацій надходять на постійній основі;		
	A.14.3.2[01]	у разі потреби розробляються попередження, рекомендації та директиви щодо внутрішньої безпеки системи;		
	A.14.3.2[02]	у разі потреби розповсюджуються попередження, рекомендації та директиви щодо внутрішньої безпеки системи;		
	A.14.3.3	директиви з безпеки впроваджуються відповідно до встановлених часових рамок.		
	Загальна оцінка реалізації вимоги 14.3			
14.4	Моніторинг системи			
	A.14.4.1[01]:	проводиться моніторинг системи з метою виявлення атак та індикаторів потенційних атак;		
	A.14.4.1[02]:	проводиться моніторинг системи на предмет виявлення неавторизованих підключень;		
	A.14.4.2:	виявляється несанкціоноване використання системи;		
	A.14.4.3[01]:	проводиться моніторинг вхідного комунікаційного трафіка з метою виявлення незвичайних або несанкціонованих дій або умов;		
	A.14.4.3[02]:	проводиться моніторинг вихідного комунікаційного трафіка з метою виявлення незвичайних або несанкціонованих дій або умов.		
	Загальна оцінка реалізації вимоги 14.4			
15.1	Політика та процедури планування безпеки			
	A.15.1.1[01]	розроблені та задокументовані політики, необхідні для виконання вимог безпеки;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.15.1.1[02]	політики, необхідні для виконання вимог безпеки, розповсюджуються серед персоналу або ролей організації;		
	A.15.1.1[03]	розроблені та задокументовані процедури, необхідні для виконання вимог безпеки;		
	A.15.1.1[04]	процедури, необхідні для виконання вимог безпеки, розповсюджуються серед персоналу або ролей організації;		
	A.15.1.2[01]	політики та процедури періодично переглядаються;		
	A.15.1.2[02]	політики та процедури періодично оновлюються.		
	Загальна оцінка реалізації вимоги 15.1			
15.2	Плани захисту інформації та персональних даних			
	A.15.2.1[01]	розроблено план захисту інформації, який визначає складові компоненти системи;		
	A.15.2.1[02]	розроблено план захисту інформації, який описує робоче середовище системи;		
	A.15.2.1[03]	розроблено план захисту інформації, який описує конкретні загрози системі, які викликають занепокоєння організації;		
	A.15.2.1[04]	розроблено план захисту інформації, який надає огляд вимог до безпеки системи;		
	A.15.2.1[05]	розроблено план захисту інформації, який визначає з'єднання з іншими системами;		
	A.15.2.1[06]	розроблено план захисту інформації, який визначає осіб, що виконують ролі та обов'язки в системі;		
	A.15.2.1[07]	розроблено план захисту інформації, який містить іншу інформацію, необхідну для захисту відкритої та конфіденційної інформації;		
	A.15.2.2[01]	план захисту інформації періодично переглядається;		
	A.15.2.2[02]	план захисту інформації періодично оновлюється;		

№ вимоги	Оцінка		Висновок з оцінки	Докази, джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.15.2.3	план захисту інформації захищено від неавторизованого розголошення.		
	Загальна оцінка реалізації вимоги 15.2			
Оцінка реалізації базового профілю				

Додаток 2
до Рекомендацій з оцінки достатності
заходів захисту інформації
комплексних систем захисту
інформації в інформаційних,
електронних комунікаційних та
інформаційно-комунікаційних
системах, створених з використанням
профілів безпеки інформації
(пункт 4 розділу III)

Рекомендації
з оцінки реалізації базового профілю безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, де обробляється службова інформація

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
1.1	Управління обліковими записами			
	A.1.1.ODP[01]	визначено період неактивності облікового запису перед відключенням;		
	A.1.1.1[01]	визначено дозволені типи облікових записів у системі;		
	A.1.1.1[02]	визначено заборонені типи облікових записів у системі;		
	A.1.1.2[01]	облікові записи створюються відповідно до політики організації, процедур, умов та критеріїв організації;		
	A.1.1.2[02]	облікові записи увімкнуто відповідно до політики організації, процедур, умов та критеріїв організації;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.1.2[03]	облікові записи модифікуються відповідно до політики, процедур, умов та критеріїв організації;		
	A.1.1.2[04]	облікові записи вимкнено відповідно до політики, процедур, умов та критеріїв організації;		
	A.1.1.2[05]	облікові записи в системі видаляються відповідно до політики, процедур, умов та критеріїв організації;		
	A.1.1.3[01]	визначено авторизованих користувачів системи;		
	A.1.1.3[02]	визначено приналежність до групи та ролі;		
	A.1.1.3[03]	визначено повноваження доступу (тобто привілеї);		
	A.1.1.4[01]	доступ до системи дозволено на основі наявного дозволу на доступ;		
	A.1.1.4[02]	доступ до системи дозволено на основі цільового використання системи;		
	A.1.1.5	проводиться моніторинг використання облікових записів у системі;		
	A.1.1.6[01]	облікові записи в системі вимикаються, коли термін дії облікових записів закінчився;		
	A.1.1.6[02]	облікові записи в системі вимкнено, якщо вони були неактивними протягом <A.1.1.ODP[01] період часу>		
	A.1.1.6[03]	облікові записи в системі вимикаються, коли облікові записи більше не пов’язані з користувачем або особою;		
	A.1.1.6[04]	облікові записи в системі вимкнено, якщо вони порушують політику організації;		
	A.1.1.6[05]	облікові записи в системі відключаються при виявленні значних ризиків, пов’язаних з фізичними особами;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.1.7[01]	співробітники або відповідні ролі організації отримують повідомлення про те, що облікові записи більше не потрібні;		
	A.1.1.7[02]	співробітники або ролі організації отримують повідомлення про звільнення;		
	A.1.1.7[03]	співробітники або ролі отримують сповіщення, коли використовується система або потрібно знати зміни для окремої особи.		
	Загальна оцінка реалізації вимоги 1.1			
1.2	Забезпечення доступу			
	A.1.2	застосовано затверджені повноваження для логічного доступу до службової інформації та ресурсів у системі.		
	Загальна оцінка реалізації вимоги 1.2			
1.3	Управління інформаційними потоками			
	A.1.3	застосовано затверджені вимоги для управління потоками службової інформації всередині системи та між підключеними системами.		
	Загальна оцінка реалізації вимоги 1.3			
1.4	Розмежування обов’язків			
	A.1.4.1	визначено обов’язки осіб, які потребують розмежування;		
	A.1.4.2	встановлено правила авторизації доступу для підтримки розмежування обов’язків.		
	Загальна оцінка реалізації вимоги 1.4			
1.5	Мінімізація повноважень			
	A.1.5.ODP[01]	визначено функції безпеки для авторизованого доступу до системи;		
	A.1.5.ODP[02]	визначено важливу для безпеки інформацію для авторизованого доступу;		
	A.1.5.1	доступ користувачів (або процесів, що діють від імені користувачів) до системи дозволено лише тоді, коли це необхідно для виконання призначених завдань;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.5.2[01]	дозволено доступ до <A.1.5.ODP[01] функцій безпеки>;		
	A.1.5.2[02]	дозволено доступ до <A.1.5.ODP[01] інформації, що стосується безпеки>.		
	A.1.5.3	періодично перевіряються привілеї, призначені ролям або класам користувачів, щоб підтвердити необхідність таких привілеїв;		
	A.1.5.4	за необхідності привілеї перепризначаються або вилучаються.		
	Загальна оцінка реалізації вимоги 1.5			
1.6	Мінімізація повноважень – непривілейований доступ до незахищених функцій			
	A.1.6.ODP[01]	визначено персонал або ролі, до яких слід обмежити привілейовані облікові записи у системі;		
	A.1.6.1	привілейовані облікові записи у системі обмежено до <A.1.6.ODP[01]: персонал або ролі>;		
	A.1.6.2	користувачі (або ролі) з привілейованими обліковими записами зобов’язані використовувати непривілейовані облікові записи для доступу до незахищених функцій або інформації.		
	Загальна оцінка реалізації вимоги 1.6			
1.7	Мінімізація повноважень – Заборона непривілейованим користувачам виконувати привілейовані функції			
	A.1.7.1	непривілейованим користувачам заборонено виконувати привілейовані функції;		
	A.1.7.2	реєструється виконання привілейованих функцій.		
	Загальна оцінка реалізації вимоги 1.7			
1.8	Невдалі спроби входу в систему			
	A.1.8.ODP[01]	визначена кількість послідовних невдалих спроб входу користувача в систему, дозволених протягом певного періоду часу;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.8.ODP[02]	визначено період часу, яким обмежено кількість послідовних невдалих спроб входу користувача;		
	A.1.8	визначено кількість послідовних невірних спроб входу користувача протягом <1.8.ODP[02]: період часу> обмежено до <A.1.8.ODP[01]: кількість>.		
	Загальна оцінка реалізації вимоги 1.8			
1.9	Попередження про використання системи			
	A.1.9	відображається повідомлення в системі з попередженнями про конфіденційність і безпеку відповідно до застосованих правил керівних документів для службової інформації перед тим, як надати доступ до системи.		
	Загальна оцінка реалізації вимоги 1.9			
1.10	Блокування пристрою			
	A.1.10.ODP[01]	вибрано одне або декілька з таких значень параметрів: {ініціювання блокування пристрою після <A.1.10.ODP[02] періоду неактивності; вимога до користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду};		
	A.1.10.ODP[02]	визначено період бездіяльності, після якого ініціюється блокування пристрою (якщо вибрано);		
	A.1.10.1	доступ до системи заборонено за <A.1.10.ODP[01]: вибране значення параметра(ів)>;		
	A.1.10.2	блокування пристрою зберігається доти, доки користувач не відновить доступ за допомогою встановлених процедур ідентифікації та автентифікації;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.10.3	інформація, яку раніше було видно на дисплеї, приховується за допомогою блокування пристрою із загальнодоступним зображенням.		
	Загальна оцінка реалізації вимоги 1.10			
1.11	Припинення сеансу			
	A.1.11.ODP[01]	визначено умови або події, які вимагають відключення сеансу;		
	A.1.11	сеанс користувача автоматично завершується після <A.1.11.ODP[01]: умови або тригерні події>.		
	Загальна оцінка реалізації вимоги 1.11			
1.12	Віддалений доступ			
	A.1.12.1[01]	визначено типи допустимого віддаленого доступу до системи;		
	A.1.12.1[02]	встановлено обмеження використання для кожного типу дозволеного віддаленого доступу до системи;		
	A.1.12.1[03]	визначено вимоги до конфігурації для кожного типу дозволеного віддаленого доступу до системи;		
	A.1.12.1[04]	для кожного типу дозволеного віддаленого доступу до системи встановлюються вимоги до підключення;		
	A.1.12.2	кожен тип віддаленого доступу до системи авторизується перед встановленням таких з’єднань;		
	A.1.12.3	віддалений доступ до системи маршрутизується через керовані точки контролю доступу;		
	A.1.12.4[01]	дозволено віддалене виконання привілейованих команд;		
	A.1.12.4[02]	дозволено віддалений доступ до інформації, важливої для безпеки.		
	Загальна оцінка реалізації вимоги 1.12			
1.13	Бездротовий доступ			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.13.1[01]	визначено кожен тип бездротового доступу до системи;		
	A.1.13.1[02]	для кожного типу бездротового доступу до системи визначено обмеження на використання;		
	A.1.13.1[03]	визначено вимоги до конфігурації для кожного типу бездротового доступу до системи;		
	A.1.13.1[04]	для кожного типу бездротового доступу до системи встановлюються вимоги до підключення;		
	A.1.13.2	кожен тип бездротового доступу до системи авторизується перед встановленням таких з'єднань;		
	A.1.13.3	вимкнено перед розгортанням та запуском бездротові мережеві можливості, якщо вони не призначені для використання.		
	Загальна оцінка реалізації вимоги 1.13			
1.14	Контроль доступу для мобільних пристроїв			
	A.1.14.1[01]	для мобільних пристроїв встановлено обмеження щодо використання;		
	A.1.14.1[02]	для мобільних пристроїв встановлено вимоги до конфігурації;		
	A.1.14.1[03]	для мобільних пристроїв встановлено вимоги до підключення;		
	A.1.14.2	дозволено підключення мобільних пристроїв до системи;		
	A.1.14.3	впроваджено повне шифрування носія інформації пристрою або шифрування на основі шифрування сховищ інформації (контейнерів) для захисту конфіденційності службової інформації на мобільних пристроях.		
	Загальна оцінка реалізації вимоги 1.14			
1.15	Використання зовнішніх систем			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.1.15.ODP[01]	визначено умови, яким повинні відповідати зовнішні системи, перш ніж дозволити використання або доступ до цих систем авторизованим особам;		
	A.1.15.ODP[02]	визначено вимоги щодо безпеки, які мають бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам;		
	A.1.15.1	використання зовнішніх систем, окрім систем, дозволених організацією;		
	A.1.15.2[01]	визначені такі умови, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам: <A.1.15.ODP[01]: умови та положення>;		
	A.1.15.2[02]	встановлюються такі вимоги безпеки, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованими особами: <A.1.15.ODP[02]: вимоги безпеки>;		
	A.1.15.3[01]	авторизованим особам дозволяється використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі службової інформації тільки після перевірки виконання вимог безпеки в зовнішній системі, як зазначено в планах безпеки організації;		
	A.1.15.3[02]	авторизованим особам дозволяється використовувати зовнішню систему для доступу до організаційної системи або для обробки, зберігання чи передачі службової інформації тільки після збереження затверджених угод про підключення або обробку даних з організацією, що розміщує		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		зовнішню систему, з якою укладено відповідну угоду;		
	A.1.15.4	обмежено використання авторизованими особами портативних пристроїв зберігання даних, контрольованих організацією, у зовнішніх системах.		
	Загальна оцінка реалізації вимоги 1.15			
1.16	Публічно доступний контент			
	A.1.16.1	авторизовані особи проходять навчання з метою нерозголошення службової інформації в загальнодоступних системах;		
	A.1.16.2[01]	вміст публічно доступного контенту періодично перевіряється на наявність службової інформації;		
	A.1.16.2[02]	видаляється відкрита та конфіденційна інформація з загальнодоступних систем у разі виявлення.		
	Загальна оцінка реалізації вимоги 1.16			
2.1	Навчання з підвищення обізнаності			
	A.2.1.ODP[01]	визначено події, які потребують навчання користувачів системи з питань безпеки;		
	A.2.1.1.1[01]	користувачам системи надається навчання з питань безпеки як частина початкового навчання для нових користувачів;		
	A.2.1.1.1[02]	навчання з питань безпеки надається користувачам системи періодично після початкового навчання;		
	A.2.1.1.2	навчання з питань безпеки проводиться для користувачів системи, коли цього вимагають зміни у системі або наступні <A.2.1.ODP[01] події>;		
	A.2.1.1.3[01]	проводиться навчання з безпеки щодо розпізнавання ознак внутрішньої загрози;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.2.1.1.3[02]	проводиться тренінги з безпекової обізнаності щодо повідомлення про ознаки внутрішньої загрози;		
	A.2.1.1.3[03]	проводиться навчання з безпекової обізнаності щодо розпізнавання індикаторів соціальної інженерії;		
	A.2.1.1.3[04]	проводиться навчання з питань безпекової обізнаності щодо розпізнавання ознак соціальної інженерії;		
	A.2.1.1.3[05]	проводиться навчання з безпекової обізнаності щодо розпізнавання ознак соціального інженерії;		
	A.2.1.1.3[06]	проводиться навчання з питань безпекової обізнаності щодо повідомлення про ознаки соціального інженерії;		
	A.2.1.2[01]	зміст тренінгу з безпекової обізнаності періодично оновлюється;		
	A.2.1.2[02]	зміст тренінгу з безпекової обізнаності оновлено після <A.2.1.ODP[01] подій>.		
	Загальна оцінка реалізації вимоги 2.1			
2.2	Рольове навчання			
	A.2.2.ODP[01]	визначено події, яких потребують тренінги з безпеки, для персоналу організації на основі покладених обов’язків;		
	A.2.2.1.1[01]	персонал організації проходить тренінги з безпеки на основі покладених обов’язків перед наданням доступу до системи або службової інформації;		
	A.2.2.1.1[02]	персонал організації проходить тренінги з безпеки на основі покладених обов’язків перед виконанням призначених обов'язків;		
	A.2.2.1.1[03]	тренінги з безпеки на основі покладених обов’язків проводяться для персоналу організації періодично після першого доступу;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.2.2.1.2	тренінги з безпеки на основі покладених обов'язків проводяться для персоналу організації, коли цього вимагають зміни в системі або після <A.2.2.ODP[01] події>;		
	A.2.2.2[01]	зміст тренінгів з безпеки на основі покладених обов'язків періодично оновлюється;		
	A.2.2.2[02]	зміст тренінгів з безпеки на основі покладених обов'язків оновлено після <A.2.2.ODP[01] подій>.		
	Загальна оцінка реалізації вимоги 2.2			
3.1	Події аудиту			
	A.3.1.ODP[01]	визначено типи подій, вибраних для реєстрації у системі;		
	A.3.1.1	визначено такі типи подій для реєстрації у системі: <A.3.1.ODP[01] типи подій>;		
	A.3.1.2[01]	періодично переглядаються типи подій, вибрані для реєстрації;		
	A.3.1.2[02]	періодично оновлюються типи подій, вибрані для реєстрації.		
	Загальна оцінка реалізації вимоги 3.1			
3.2	Зміст записів аудиту			
	A.3.2.1.[01]:	записи аудиту містять інформацію, яка дозволяє встановити, який тип події стався;		
	A.3.2.1.[02]:	записи аудиту містять інформацію, яка дозволяє встановити, коли відбулася подія;		
	A.3.2.1.[03]:	записи аудиту містять інформацію, яка встановлює, де відбулася подія;		
	A.3.2.1.[04]:	записи аудиту містять інформацію, яка встановлює джерело події;		
	A.3.2.1.[05]:	записи аудиту містять інформацію, яка встановлює результат події;		
	A.3.2.1.[06]:	записи аудиту містять інформацію, що встановлює особу, суб'єкта, об'єкта або організацію, пов'язану з подією;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.3.2.2:	додаткова інформація для записів аудиту надається у разі потреби.		
	Загальна оцінка реалізації вимоги 3.2			
3.3	Збереження записів аудиту			
	A.3.3.1	згенеровано записи аудиту для вибраних типів подій і згідно з вмістом записів аудиту, вказаних в 3.1 та в 3.2;		
	A.3.3.2	записи аудиту зберігаються протягом періоду часу, який відповідає політиці зберігання записів аудиту.		
	Загальна оцінка реалізації вимоги 3.3			
3.4	Реагування на відмови обробки даних аудиту			
	A.3.4.ODP[01]	визначено період часу, протягом якого персонал організації або ролі отримують сповіщення у разі відмови обробки даних аудиту;		
	A.3.4.ODP[02]	визначено додаткові дії, які слід виконати у разі відмови обробки даних аудиту;		
	A.3.4.1	персонал або ролі організації отримують сповіщення у разі відмови в процесі обробки даних аудиту в межах <A.3.4.ODP[01] періоду часу>;		
	A.3.4.2	наступні додаткові дії виконуються у разі відмови в процесі реєстрації аудиту: <A.3.4.ODP[02] додаткові дії>.		
	Загальна оцінка реалізації вимоги 3.4			
3.5	Огляд, аналіз і звітність аудиту			
	A.3.5.1	записи аудиту системи періодично переглядаються та аналізуються на предмет виявлення ознак та потенційного впливу не властивої або незвичної діяльності;		
	A.3.5.2	результати аудиту доводяться до відома співробітникам організації або ролям;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.3.5.3	записи аудиту в різних сховищах аналізуються та зіставляються задля забезпечення ситуативної обізнаності в масштабах організації.		
	Загальна оцінка реалізації вимоги 3.5			
3.6	Скорочення записів аудиту та формування звіту			
	A.3.6.1	впроваджено функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, вимоги до звітності та постфактум розслідування інцидентів;		
	A.3.6.2	збережено оригінальний зміст і часовий порядок записів аудиту.		
	Загальна оцінка реалізації вимоги 3.6			
3.7	Позначка часу			
	A.3.7.ODP[01]	визначено деталізацію вимірювання часу для позначок часу записів аудиту;		
	A.3.7.1	використовується внутрішній годинник у системі для генерування позначок часу записів аудиту;		
	A.3.7.2[01]	відповідають позначки часу для записів аудиту <A.3.7.ODP[01] деталізація вимірювання часу>;		
	A.3.7.2[02]	позначки часу для записів аудиту використовують всесвітній координований час (UTC), мають фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу як частину позначки часу.		
	Загальна оцінка реалізації вимоги 3.7			
3.8	Захист інформації аудиту			
	A.3.8.1	інформація аудиту та інструменти журналювання аудиту захищені від несанкціонованого доступу, модифікації та видалення;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.3.8.2	доступ до управління функціями аудиту дозволено лише підмножині привілейованих користувачів або ролей.		
	Загальна оцінка реалізації вимоги 3.8			
4.1	Базова конфігурація			
	A.4.1.1[01]	розроблено поточну базову конфігурацію системи;		
	A.4.1.1[02]	підтримується поточна базова конфігурація системи під контролем конфігурації;		
	A.4.1.2[01]	періодично переглядається базова конфігурація системи;		
	A.4.1.2[02]	переглядається базова конфігурація системи при встановленні або модифікації компонентів системи;		
	A.4.1.2[03]	періодично оновлюється базова конфігурація системи;		
	A.4.1.2[04]	оновлюється базова конфігурація системи, коли встановлюються або змінюються компоненти системи.		
	Загальна оцінка реалізації вимоги 4.1			
4.2	Налаштування конфігурації			
	A.4.2.ODP[01]	визначено параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам;		
	A.4.2.1[01]	визначено та задокументовано такі параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: <A.4.2.ODP[01] налаштування конфігурації>;		
	A.4.2.1[02]	реалізовано такі налаштування конфігурації системи: <A.4.2.ODP[01] налаштування конфігурації>;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.2.2[01]	визначено та задокументовано будь-які відхилення від встановлених параметрів конфігурації;		
	A.4.2.2[02]	затверджено всі відхилення від встановлених налаштувань конфігурації.		
	Загальна оцінка реалізації вимоги 4.2			
4.3	Управління змінами конфігурації			
	A.4.3.1	визначено типи змін у конфігурації системи, які необхідно контролювати;		
	A.4.3.2[01]	переглядаються запропоновані зміни в конфігурації системи, які необхідно контролювати;		
	A.4.3.2[02]	запропоновані зміни в конфігурації системи схвалюються або відхиляються з урахуванням впливу на безпеку;		
	A.4.3.3[01]	впроваджуються затверджені зміни в конфігурації системи, які необхідно контролювати;		
	A.4.3.3[02]	задокументовані затверджені зміни в конфігурації системи, які необхідно контролювати;		
	A.4.3.4[01]	відстежуються дії, пов'язані зі змінами конфігурації системи, які необхідно контролювати;		
	A.4.3.4[02]	переглядаються дії, пов'язані зі змінами конфігурації системи, які необхідно контролювати.		
	Загальна оцінка реалізації вимоги 4.3			
4.4	Аналіз впливу на безпеку та приватність			
	A.4.4	проводиться аналіз впливу змін у системі на безпеку перед їх впровадженням.		
	Загальна оцінка реалізації вимоги 4.4			
4.5	Обмеження доступу до змін			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.5[01]	визначено та задокументовано фізичні та логічні обмеження доступу, пов'язані зі змінами в системі;		
	A.4.5[02]	затверджені обмеження фізичного доступу, пов'язані зі змінами в системі;		
	A.4.5[03]	застосовуються обмеження фізичного доступу, пов'язані зі змінами в системі;		
	A.4.5[04]	визначені та задокументовані логічні обмеження доступу, пов'язані зі змінами в системі;		
	A.4.5[05]	затверджені логічні обмеження доступу, пов'язані зі змінами в системі;		
	A.4.5[06]	введено в дію логічні обмеження доступу, пов'язані зі змінами в системі.		
	Загальна оцінка реалізації вимоги 4.5			
4.6	Мінімально необхідна функціональність			
	A.4.6.ODP[01]	визначено функції, які потрібно заборонити або обмежити;		
	A.4.6.ODP[02]	визначено порти, які потрібно заборонити або обмежити;		
	A.4.6.ODP[03]	визначено протоколи, які потрібно заборонити або обмежити;		
	A.4.6.ODP[04]	визначено з'єднання, які потрібно заборонити або обмежити;		
	A.4.6.ODP[05]	визначено служби, які потрібно заборонити або обмежити;		
	A.4.6.ODP[06]	визначено функції, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[07]	визначено порти, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[08]	визначено протоколи, які вважаються непотрібними або небезпечними;		
	A.4.6.ODP[09]	визначено з'єднання, які вважаються непотрібними або небезпечними;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.6.ODP[10]	визначено служби, які вважаються непотрібними або небезпечними;		
	A.4.6.1	система налаштована на надання лише необхідних для виконання завдань і функцій;		
	A.4.6.2[01]	заборонено або обмежено використання таких функцій: <A.4.6.ODP[01]: функції>;		
	A.4.6.2[02]	заборонено або обмежено використання таких портів: <A.4.6.ODP[02]: порти>;		
	A.4.6.2[03]	використання таких протоколів заборонено або обмежено: <A.4.6.ODP[03]: протоколи>;		
	A.4.6.2[04]	заборонено або обмежено використання таких з'єднань: <A.4.6.ODP[04]: з’єднання>;		
	A.4.6.2[05]	заборонено або обмежено використання таких служб: <A.4.6.ODP[05]: служби>;		
	A.4.6.3	система періодично переглядається для виявлення непотрібних або небезпечних функцій, портів, протоколів, з'єднань і служб;		
	A.4.6.4[01]	вимкнено або видалено такі непотрібні або небезпечні функції: <A.4.6.ODP[06]: функції>;		
	A.4.6.4[02]	вимкнено або вилучено такі непотрібні або небезпечні порти: <A.4.6.ODP[07]: порти>;		
	A.4.6.4[03]	вимкнено або вилучено такі непотрібні або небезпечні протоколи: <A.4.6.ODP[08]: протоколи>;		
	A.4.6.4[04]	вимкнено або видалено такі непотрібні або небезпечні з'єднання: <A.4.6.ODP[09]: з’єднання>;		
	A.4.6.4[05]	вимкнено або вилучено такі непотрібні або небезпечні служби: <A.4.6.ODP[10]: служби>.		
	Загальна оцінка реалізації вимоги 4.6			
4.7	Мінімально необхідна функціональність – Авторизоване програмне забезпечення – Чорний список			
	A.4.7.1	визначено програми, яким дозволено виконуватись в системі;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.7.2	впроваджено політику "заборонити все", "дозволити за винятком" для виконання програм у системі;		
	A.4.7.3[01]	періодично переглядається список дозволеного програмного забезпечення;		
	A.4.7.3[02]	періодично оновлюється список дозволеного програмного забезпечення;		
	Загальна оцінка реалізації вимоги 4.7			
4.8	Інвентаризація компонентів системи			
	A.4.8.1	розроблено та задокументовано перелік компонентів системи;		
	A.4.8.2[01]	перелік компонентів системи періодично переглядається;		
	A.4.8.2[02]	перелік компонентів системи оновлюється;		
	A.4.8.3[01]	перелік компонентів системи оновлюється під час інсталяції;		
	A.4.8.3[02]	перелік компонентів системи оновлено під час видалення компонентів;		
	A.4.8.3[03]	перелік компонентів системи оновлено під час оновлення системи.		
	Загальна оцінка реалізації вимоги 4.8			
4.9	Розташування інформації			
	A.4.9.1[01]	визначено та задокументовано розташування службової інформації;		
	A.4.9.1[02]	визначено та задокументовано компоненти системи, на яких обробляється службова інформація;		
	A.4.9.1[03]	компоненти системи, на яких зберігається службова інформація, ідентифіковано та задокументовано;		
	A.4.9.2[01]	ідентифіковано та задокументовано користувачів, які мають доступ до системи та компонентів системи, де обробляється службова інформація;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.4.9.2[02]	ідентифіковано та задокументовано користувачів, які мають доступ до системи та компонентів системи, де зберігається службова інформація;		
	A.4.9.3[01]	задокументовано зміни в розташуванні (тобто в системі або компонентах системи), де обробляється службова інформація;		
	A.4.9.3[02]	задокументовано зміни в розташуванні (тобто в системі або компонентах системи), де зберігається службова інформація.		
	Загальна оцінка реалізації вимоги 4.9			
4.10	Базова конфігурація – Конфігурація системи та компонентів для сфер з високим ризиком			
	A.4.10.ODP[01]	системи або компоненти системи з такими конфігураціями видаються особам, які відряджаються до місць підвищеного ризику;		
	A.4.10.ODP[02]	визначено вимоги безпеки до системи та компонентів системи після повернення осіб з відрядження;		
	A.4.10.1	системи або компоненти системи з такими конфігураціями видаються особам, які відряджаються до місць підвищеного ризику: <A.4.10.ODP[01]: системи>;		
	A.4.10.2	застосовуються вимоги безпеки до системи та компонентів системи після повернення осіб з відрядження:<A.4.10.ODP[02]: вимоги>.		
	Загальна оцінка реалізації вимоги 4.10			
5.1	Ідентифікація та автентифікація (користувачів організації)			
	A.5.1.ODP[01]	визначено обставини або ситуації, які вимагають повторної автентифікації;		
	A.5.1.1[01]	користувачі системи унікально ідентифіковані та автентифіковані;		
	A.5.1.1[02]	унікальна ідентифікація автентифікованих користувачів системи пов'язана з процесами, що діють від імені цих користувачів.		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.5.1.2	користувачі проходять повторну автентифікацію, коли <A.5.1.ODP[01]: обставини або ситуацій>.		
	Загальна оцінка реалізації вимоги 5.1			
5.2	Ідентифікація та автентифікація пристроїв			
	A.5.2	пристрої унікально ідентифікуються та автентифікуються перед встановленням з'єднання із системою.		
	Загальна оцінка реалізації вимоги 5.2			
5.3	Ідентифікація та автентифікація (користувачів організації) – багатофакторна автентифікація привілейованих облікових записів			
	A.5.3	реалізовано багатофакторну автентифікацію для доступу до облікових записів системи.		
	Загальна оцінка реалізації вимоги 5.3			
5.4	Ідентифікація та автентифікація (користувачів організації) – доступ до облікових записів – стійкість до відтворення			
	A.5.4	реалізовано стійкі до повторного відтворення механізми автентифікації для доступу до облікових записів у системі.		
	Загальна оцінка реалізації вимоги 5.4			
5.5	Управління ідентифікацією			
	A.5.5.ODP[01]	визначено персонал або ролі, від яких необхідно отримати дозвіл на призначення ідентифікатора;		
	A.5.5.ODP[02]	визначено період часу для запобігання повторному використанню ідентифікаторів;		
	A.5.5.1	отримано дозвіл від <A.5.5.ODP[01]: персонал або ролі> на призначення ідентифікатора особи, групи, ролі, служби або пристрою;		
	A.5.5.2[01]	вибрано ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій;		
	A.5.5.2[02]	призначено ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій;		
	A.5.5.3	запобігання повторному використанню ідентифікаторів для <A.5.5.ODP[02]: період часу>;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.5.5.4	статус кожної особи унікально ідентифікується за допомогою ідентифікаційної характеристики;		
	Загальна оцінка реалізації вимоги 5.5			
5.6	Управління автентифікатором – автентифікація на основі пароля			
	A.5.6.ODP[01]	правила складу та складності паролів;		
	A.5.6.1[01]	ведеться список часто використовуваних, очікуваних або скомпрометованих паролів;		
	A.5.6.1[02]	періодично оновлюється список часто використовуваних, очікуваних або скомпрометованих паролів;		
	A.5.6.1[03]	оновлюється список часто використовуваних, очікуваних або скомпрометованих паролів у разі виникнення підозри, що паролі організації були скомпрометовані;		
	A.5.6.2	перевіряються паролі на відсутність у списку часто використовуваних, очікуваних або скомпрометованих паролів, коли вони створюються або оновлюються користувачами;		
	A.5.6.3	передаються паролі лише криптографічно захищеними каналами;		
	A.5.6.4	зберігаються паролі у криптографічно захищеному вигляді;		
	A.5.6.5	буде обрано новий пароль під час першого використання після відновлення облікового запису;		
	A.5.6.6	виконуються такі правила складу та складності: <A.5.6.ODP[01]: правила>.		
	Загальна оцінка реалізації вимоги 5.6			
5.7	Зворотний зв'язок автентифікатора			
	A.5.7.1	прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.		
	Загальна оцінка реалізації вимоги 5.7			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
5.8	Управління автентифікатором			
	A.5.8.ODP[01]	визначені події, які викликають зміну або оновлення автентифікаторів;		
	A.5.8.1	перевірено ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора;		
	A.5.8.2	встановлено початковий вміст автентифікатора для всіх автентифікаторів, виданих організацією;		
	A.5.8.3[01]	створені та впроваджені адміністративні процедури для початкового розподілу автентифікаторів;		
	A.5.8.3[02]	створені та впроваджені адміністративні процедури для втрачених, скомпрометованих або пошкоджених автентифікаторів;		
	A.5.8.3[03]	створені та впроваджені адміністративні процедури для відкликання автентифікаторів;		
	A.5.8.4	потрібно змінювати автентифікатори за замовчуванням при першому використанні;		
	A.5.8.5	потрібно періодично змінювати та оновлювати автентифікатори або коли відбуваються такі події: <A.5.8.ODP[01]: події >;		
	A.5.8.6[01]	захищено вміст автентифікатора від несанкціонованого розкриття;		
	A.5.8.6[02]	захищено вміст автентифікатора від несанкціонованої модифікації.		
	Загальна оцінка реалізації вимоги 5.8			
6.1	Обробка інциденту			
	A.6.1.1	розроблено план реагування на інциденти, який забезпечить організацію стратегією для реалізації її можливостей реагування на інциденти;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.6.1.2[01]	впроваджено систему реагування на інциденти, яка відповідає плану реагування на інциденти;		
	A.6.1.2[02]	передбачено підготовку до реагування на інциденти;		
	A.6.1.2[03]	передбачає систему реагування на інциденти, виявлення та аналіз інцидентів;		
	A.6.1.2[04]	передбачає систему реагування на інциденти, локалізацію інцидентів;		
	A.6.1.2[05]	передбачає систему реагування на інциденти, ліквідацію наслідків інцидентів;		
	A.6.1.2[06]	передбачає систему реагування на інциденти, відновлення після інцидентів;		
	A.6.1.3	оновлюється план реагування на інциденти, щоб врахувати зміни в системі та зміни в організації або проблеми, що виникли під час впровадження, виконання або тестування плану.		
	Загальна оцінка реалізації вимоги 6.1			
6.2	Моніторинг інциденту			
	A.6.2.ODP[01]	визначено період часу, протягом якого необхідно повідомляти про підозрілі інциденти до служби реагування на інциденти;		
	A.6.2.ODP[02]	визначені органи, яким слід повідомляти інформацію про інцидент;		
	A.6.2.1[01]	відстежуються інциденти, пов'язані з безпекою системи;		
	A.6.2.1[02]	документуються інциденти, пов'язані з безпекою системи;		
	A.6.2.2	повідомляється про підозрілі інциденти до служби реагування на інциденти в організації протягом <A.6.2.ODP[01]: період часу>;		
	A.6.2.3	надсилається інформація про інцидент до <A.6.2.ODP[02]: органів влади>;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.6.2.4	надається підтримка реагування на інциденти, який пропонує поради та допомогу користувачам системи щодо обробки та звітування про інциденти.		
	Загальна оцінка реалізації вимоги 6.2			
6.3	Перевірка реагувань на інциденти			
	A.6.3	проводиться періодична перевірка ефективності системи реагування на інциденти.		
	Загальна оцінка реалізації вимоги 6.3			
6.4	Навчання з реагування на інциденти			
	A.6.4.ODP[01]	визначено період часу, протягом якого користувачі системи повинні пройти навчання з реагування на інциденти;		
	A.6.4.ODP[02]	визначені події, які ініціюють перегляд та оновлення змісту навчання з реагування на інциденти;		
	A.6.4.1.[01]	проводиться навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків протягом <A.6.4.ODP[01]: період часу> після прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до системи;		
	A.6.4.1.[02]	навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків проводиться тоді, коли цього вимагають зміни в системі;		
	A.6.4.1.[03]	навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків проводиться періодично після початкового навчання та навчання, орієнтованого на конкретні події;		
	A.6.4.2[01]	проводиться періодичний перегляд змісту навчання з реагування на інциденти;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.6.4.2[02]	переглядається зміст навчання з реагування на інциденти після <A.6.4.ODP[02]: події>;		
	A.6.4.2[03]	зміст навчання з реагування на інциденти періодично оновлюється;		
	A.6.4.2[04]	зміст навчання з реагування на інциденти оновлюється після <A.6.4.ODP[02]: події>.		
	Загальна оцінка реалізації вимоги 6.4			
7.1	Інструменти для обслуговування			
	A.7.1.1[01]	затверджується використання інструментів для обслуговування системи;		
	A.7.1.1[02]	контролюється використання інструментів для обслуговування системи;		
	A.7.1.1[03]	відстежується використання інструментів для обслуговування системи;		
	A.7.1.2	перевіряються інструменти для технічного обслуговування на предмет неналежних або несанкціонованих модифікацій;		
	A.7.1.3	перевіряються носії, що містять діагностичні та тестові програми, на наявність шкідливого коду перед використанням у системі;		
	A.7.1.4	можливо запобігти вилученню обладнання для обслуговування системи, що містить службову інформацію, шляхом перевірки відсутності службової інформації на обладнанні; процедури очистки або знищення обладнання; або збереження обладнання в межаї об'єкта.		
	Загальна оцінка реалізації вимоги 7.1			
7.2	Віддалене обслуговування			
	A.7.2.1[01]	дозволені віддалені сеанси з технічного обслуговування та діагностики;		
	A.7.2.1[02]	проводиться моніторинг віддалених сеансів з технічного обслуговування та діагностики;		
	A.7.2.2	реалізована багатофакторна автентифікація та стійкість до повторного відтворення при		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		створенні віддалених сеансів технічного обслуговування та діагностики;		
	A.7.2.3[01]	завершуються сеансові з'єднання після завершення віддаленого технічного обслуговування;		
	A.7.2.3[02]	розриваються мережеві з'єднання після завершення віддаленого технічного обслуговування.		
	Загальна оцінка реалізації вимоги 7.2			
7.3	Технічний персонал			
	A.7.3.1	запроваджено процес авторизації персоналу з технічного обслуговування;		
	A.7.3.2	ведеться список уповноважених організацій або персоналу з технічного обслуговування;		
	A.7.3.3	проводиться перевірка персоналу без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ;		
	A.7.3.4	призначається персонал організації з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю персоналу з технічного обслуговування, який не має необхідних повноважень доступу.		
	Загальна оцінка реалізації вимоги 7.3			
8.1	Зберігання носіїв інформації			
	A.8.1[01]	здійснюється фізичний контроль носіїв інформації, що містять відкриту та конфіденційну інформацію, до моменту їх знищення або очищення за допомогою затвердженого обладнання, методів і процедур;		
	A.8.1[02]	надійно зберігаються носії інформації, що містять відкриту та конфіденційну інформацію, до моменту їх знищення або очищення за		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		допомогою затвердженого обладнання, методів і процедур.		
	Загальна оцінка реалізації вимоги 8.1			
8.2	Доступ до носіїв інформації			
	А.8.2	обмежено доступ до службової інформації на носіях інформації.		
	Загальна оцінка реалізації вимоги 8.2			
8.3	Знищення інформації на носіях інформації			
	А.8.3	проходять очищення носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією, виходом з-під контролю організації або перед повторним використанням.		
	Загальна оцінка реалізації вимоги 8.3			
8.4	Маркування носіїв інформації			
	А.8.4[01]	на носіях інформації, що містять відкриту та конфіденційну інформацію, наявне маркування, що вказує на обмеження розповсюдження;		
	А.8.4[02]	на носіях інформації, що містять відкриту та конфіденційну інформацію, наявне маркування щодо застережень поводження з ними;		
	А.8.4[03]	на носіях інформації, що містять відкриту та конфіденційну інформацію, наявне маркування щодо позначок безпеки.		
	Загальна оцінка реалізації вимоги 8.4			
8.5	Транспортування носіїв інформації			
	А.8.5.1[01]	носії інформації, що містять відкриту та конфіденційну інформацію, захищені під час транспортування за межі контрольованих територій;		
	А.8.5.1[02]	носії інформації, що містять відкриту та конфіденційну інформацію, контролюються під час транспортування за межі контрольованих територій;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.8.5.2	зберігається облік носіїв інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій;		
	A.8.5.3	застосовуються криптографічні механізми для запобігання несанкціонованому доступу до службової інформації, що зберігається на носіях інформації, під час транспортування.		
	Загальна оцінка реалізації вимоги 8.5			
8.6	Використання носіїв інформації			
	A.8.6.ODP[01]	визначено типи носіїв інформації, використання яких обмежено або заборонено;		
	A.8.6.1	обмежено або заборонено використання таких типів носіїв інформації: <A.8.6.ODP[01]: типи носіїв інформації>;		
	A.8.6.2	заборонено використання знімних носіїв інформації без ідентифікованого власника.		
	Загальна оцінка реалізації вимоги 8.6			
8.7	Резервне копіювання - криптографічний захист			
	A.8.7	реалізовано криптографічні механізми для запобігання несанкціонованому розкриттю службової інформації в місцях зберігання резервних копій.		
	Загальна оцінка реалізації вимоги 8.7			
9.1	Перевірка персоналу			
	A.9.1.ODP[01]	визначено умови, які вимагають повторної перевірки осіб;		
	A.9.1.1	особи проходять перевірку перед наданням доступу до системи;		
	A.9.1.2	особи проходять повторну перевірку відповідно до наведених нижче умов: <A.9.1.ODP[01]: умови>.		
	Загальна оцінка реалізації вимоги 9.1			
9.2	Звільнення персоналу. Переведення персоналу			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.9.2.ODP[01]	визначено період часу, протягом якого забороняється доступ до системи;		
	A.9.2.ODP[02]	визначено період часу, протягом якого мають бути виконані дії з переведення або призначення;		
	A.9.2.ODP[03]	визначені дії з переведення або призначення;		
	A.9.2.1[01]	після припинення індивідуальної трудової діяльності доступ до системи забороняється протягом <A.9.2.ODP[01]: період часу>;		
	A.9.2.1[02]	після припинення індивідуальної трудової діяльності припиняються або відкликаються пов'язані з нею автентифікатори та облікові дані;		
	A.9.2.1[03]	після припинення індивідуальної трудової діяльності відновлюються властивості системи, пов’язані із системою;		
	A.9.2.2[01]	при перепризначенні або переведенні працівників на інші посади в організації переглядаються та підтверджуються поточні оперативні потреби в поточних логічних та фізичних правах доступу до системи та об'єкта;		
	A.9.2.2[02]	при перепризначенні або переведенні працівників на інші посади в організації ініціюються <A.9.2.ODP[03]: дії з переведення або перепризначення> протягом <A.9.2.ODP[02]: період часу>;		
	A.9.2.2[03]	при перепризначенні або переведенні працівників на інші посади в організації повноваження доступу змінюються відповідно до будь-яких змін в оперативних потребах.		
	Загальна оцінка реалізації вимоги 9.2			
10.1	Авторизація фізичного доступу			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.10.1.1[01]	розроблено список осіб, які мають право доступу до фізичного місця розташування системи;		
	A.10.1.1[02]	затверджено список осіб, які мають право доступу до фізичного місця розташування системи;		
	A.10.1.1[03]	підтримується список осіб, які мають право доступу до фізичного місця розташування системи;		
	A.10.1.2	надаються повноваження для доступу до об'єкта;		
	A.10.1.3	список фізичного доступу періодично перевіряється;		
	A.10.1.4	особи видаляються зі списку фізичного доступу, коли доступ більше не потрібен.		
	Загальна оцінка реалізації вимоги 10.1			
10.2	Моніторинг фізичного доступу			
	A.10.2.1[01]	проводиться моніторинг фізичного доступу до місця розташування системи для виявлення інцидентів фізичної безпеки;		
	A.10.2.1[02]	проводиться моніторинг фізичного доступу до місця розташування системи для реагування на інциденти фізичної безпеки;		
	A.10.2.2	журнали фізичного доступу періодично переглядаються.		
	Загальна оцінка реалізації вимоги 10.2			
10.3	Альтернативне робоче місце			
	A.10.3.ODP[01]	визначено вимоги безпеки, які необхідно дотримуватися на альтернативних робочих місцях;		
	A.10.3.1	визначені альтернативні робочі місця, дозволені для використання працівниками;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.10.3.2	на альтернативних робочих місцях застосовуються такі вимоги безпеки: <A.10.3.ODP[01]: вимоги безпеки>.		
	Загальна оцінка реалізації вимоги 10.3			
10.4	Керування фізичним доступом			
	A.10.4.ODP[01]	визначено обставини, що вимагають супроводу відвідувачів і контролю за їх діяльністю;		
	A.10.4.1[01]	фізичний доступ контролюється в місці розташування системи шляхом перевірки індивідуальних дозволів на фізичний доступ перед здійсненням доступу;		
	A.10.4.1[02]	фізичний доступ контролюється в місці розташування системи шляхом контролю входу та виходу за допомогою систем/пристроїв контролю фізичного доступу або охоронців;		
	A.10.4.2	ведуться журнали контролю фізичного доступу для точок входу та виходу;		
	A.10.4.3[01]	відвідувачі супроводжуються;		
	A.10.4.3[02]	діяльність відвідувачів контролюється за таких обставин: <A.10.4.ODP[01]: обставини>;		
	A.10.4.4[01]	забезпечений захист ключів;		
	A.10.4.4[02]	забезпечений захист кодів;		
	A.10.4.4[03]	забезпечений захист інших пристроїв фізичного доступу.		
	Загальна оцінка реалізації вимоги 10.4			
10.5	Контроль доступу до джерел і ліній електроживлення. Контроль доступу до пристроїв виведення інформації			
	A.10.5.1	контролюється фізичний доступ до розподільчих ліній системи та ліній електропередач на об'єктах організації;		
	A.10.5.2	фізичний доступ до пристроїв виведення контролюється, щоб запобігти доступу сторонніх осіб до службової інформації.		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 10.5			
11.1	Оцінювання ризику			
	A.11.1.1	оцінюється ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі конфіденційної інформації;		
	A.11.1.2	оцінювання ризиків періодично оновлюється.		
	Загальна оцінка реалізації вимоги 11.1			
11.2	Сканування вразливостей			
	A.11.2.ODP[01]	визначено час на реагування для усунення вразливостей системи;		
	A.11.2.1[01]	система періодично перевіряється на наявність вразливостей;		
	A.11.2.1[02]	система відстежується на наявність вразливостей, коли виявляються нові вразливості, що впливають на систему;		
	A.11.2.1[03]	система періодично сканується на наявність вразливостей;		
	A.11.2.1[04]	система сканується на вразливості при виявленні нових вразливостей, які впливають на систему;		
	A.11.2.2	усуваються вразливості системи протягом <A.11.2.ODP[01]: час на реагування>;		
	A.11.2.3[01]	періодично оновлюється список вразливостей системи для сканування;		
	A.11.2.3[02]	список вразливостей системи, що підлягають скануванню, оновлюються при виявленні нових вразливостей;		
	A.11.2.3[03]	список вразливостей системи, що підлягають скануванню, оновлюються, коли повідомляється про нові вразливості.		
	Загальна оцінка реалізації вимоги 11.2			
12.1	Оцінювання			
	A.12.1	вимоги до захисту інформації в системі та середовища її функціонування періодично		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		оцінюються для визначення того, чи були виконані ці вимоги.		
	Загальна оцінка реалізації вимоги 12.1			
12.2	План усунення недоліків і контрольні показники			
	A.12.2.1[01]	розроблено план дій і контрольні показники з метою документування запланованих заходів з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки;		
	A.12.2.1[02]	розроблено план дій і контрольні показники з метою зменшення або усунення відомих недоліків системи;		
	A.12.2.2[01]	існуючий план дій і контрольні показники періодично оновлюються на основі результатів оцінки безпеки;		
	A.12.2.2[02]	існуючий план дій і контрольні показники періодично оновлюються на основі результатів незалежних аудитів або оглядів;		
	A.12.2.2[03]	існуючий план дій і контрольні показники періодично оновлюються на основі результатів безперервного моніторингу.		
	Загальна оцінка реалізації вимоги 12.2			
12.3	Безперервний моніторинг			
	A.12.3[01]	розроблено та впроваджено стратегію безперервного моніторингу на рівні системи;		
	A.12.3[02]	постійний моніторинг внесений до стратегії безперервного моніторингу;		
	A.12.3[03]	оцінка безпеки внесена до стратегії безперервного моніторингу.		
	Загальна оцінка реалізації вимоги 12.3			
12.4	Взаємодія систем			
	A.12.4.ODP[01]	вибрано одне або декілька з наступних значень параметрів: {угоди про безпеку з'єднання; угоди про безпеку обміну інформацією; меморандуми або угоди про взаєморозуміння;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		угоди про рівень обслуговування; угоди з користувачами; угоди про нерозголошення інформації};		
	A.12.4.1	обмін відкритою та конфіденційною інформацією між системою та іншими системами затверджено та керується за допомогою <A.12.4.ODP[01]: вибране значення параметра(ів)>;		
	A.12.4.2[01]	характеристики інтерфейсу задокументовані як частина договорів про обмін;		
	A.12.4.2[02]	вимоги до безпеки задокументовані як частина договорів про обмін;		
	A.12.4.2[03]	обов'язки для кожної системи задокументовані як частина договорів про обмін;		
	A.12.4.3[01]	договори про обмін періодично переглядаються;		
	A.12.4.3[02]	договори про обмін періодично оновлюються.		
	Загальна оцінка реалізації вимоги 12.4			
13.1	Захист периметра			
	A.13.1.1[01]	здійснюється контроль зв’язку на зовнішніх периметрах системи;		
	A.13.1.1[02]	здійснюється управління зв’язком на зовнішніх периметрах системи;		
	A.13.1.1[03]	здійснюється контроль зв’язку на ключових внутрішніх периметрах системи;		
	A.13.1.1[04]	здійснюється управління зв’язком на ключових внутрішніх периметрах системи;		
	A.13.1.2	підмережі реалізовані для загальнодоступних компонентів системи, які фізично або логічно відділені від внутрішніх мереж;		
	A.13.1.3	підключення до зовнішніх систем здійснюється лише через керовані інтерфейси, які складаються з пристроїв захисту периметра,		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		розташованих відповідно до архітектури безпеки організації.		
	Загальна оцінка реалізації вимоги 13.1			
13.2	Інформація в загальних ресурсах системи			
	A.13.2[01]	запобігли несанкціонованій передачі інформації за допомогою загальних ресурсів системи;		
	A.13.2[02]	запобігли ненавмисній передачі інформації за допомогою загальних ресурсів системи.		
	Загальна оцінка реалізації вимоги 13.2			
13.3	Захист периметра - відмова за замовчуванням - дозвіл за винятком			
	A.13.3[01]	за замовчуванням заборонено трафік мережевих комунікацій;		
	A.13.3[02]	трафік мережевих комунікацій дозволено за винятком.		
	Загальна оцінка реалізації вимоги 13.3			
13.4	Конфіденційність і цілісність передачі. Захист інформації в стані спокою			
	A.13.4[01]	реалізовано механізми криптографічного захисту для запобігання несанкціонованому розкриттю службової інформації під час передачі;		
	A.13.4[02]	реалізовано механізми криптографічного захисту для запобігання несанкціонованому розкриттю службової інформації під час зберігання.		
	Загальна оцінка реалізації вимоги 13.4			
13.5	Відключення мережі			
	A.13.5:	мережеві з'єднання, пов'язані із сеансами зв'язку, завершуються в кінці сеансів або після періодів бездіяльності.		
	Загальна оцінка реалізації вимоги 13.5			
13.6	Встановлення та управління криптографічними ключами			
	A.13.6.ODP[01]	визначено вимоги до встановлення та управління ключами;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.13.6[01]	криптографічні ключі встановлюються в системі відповідно до таких вимог до управління ключами: <A.13.6.ODP[01]: вимоги>;		
	A.13.6[02]	управління криптографічними ключами в системі здійснюється відповідно до таких вимог до управління ключами: <A.13.6.ODP[01]: вимоги>.		
	Загальна оцінка реалізації вимоги 13.6			
13.7	Криптографічний захист			
	A.13.7.ODP[1]:	визначено типи криптографії для захисту конфіденційності службової інформації;		
	A.13.7:	для захисту конфіденційності службової інформації при використанні системи впроваджено такі типи криптографії: <A.13.7.ODP[1]: типи криптографії>.		
	Загальна оцінка реалізації вимоги 13.7			
13.8	Спільні обчислювальні пристрої та застосунки			
	A.13.8.1	заборонено віддалено активувати спільні обчислювальні пристрої та програмне забезпечення;		
	A.13.8.2	чіткі вказівки щодо використання надаються користувачам, які фізично присутні біля пристроїв.		
	Загальна оцінка реалізації вимоги 13.8			
13.9	Мобільний код			
	A.13.9.1[01]	визначено прийнятний мобільний код;		
	A.13.9.1[02]	визначено прийнятні технології мобільного коду;		
	A.13.9.2[01]	використання мобільного коду авторизовано;		
	A.13.9.2[02]	відстежується використання мобільного коду;		
	A.13.9.2[03]	контролюється використання мобільного коду.		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 13.9			
13.10	Автентифікація сесії			
	A.13.10	автентифікацію сеансів зв'язку захищено.		
	Загальна оцінка реалізації вимоги 13.10			
14.1	Виправлення дефектів			
	A.14.1.ODP[01]	визначено період часу, протягом якого слід встановити оновлення програмного забезпечення, що стосується безпеки, після випуску оновлення;		
	A.14.1.ODP[02]	визначено період часу, протягом якого слід встановити оновлення вбудованого програмного забезпечення, що стосується безпеки, після випуску оновлення;		
	A.14.1.1[01]	виявляються недоліки системи;		
	A.14.1.1[02]	повідомляється про недоліки системи;		
	A.14.1.1[03]	виправляються недоліки системи;		
	A.14.1.2[01]	оновлення програмного забезпечення, що стосується безпеки, встановлюється протягом <A.14.1.ODP[01]: періоду часу> після випуску оновлення;		
	A.14.1.2[02]	оновлення вбудованого програмного забезпечення, що стосується безпеки, встановлюється протягом <A.14.1.ODP[02]: періоду часу> після випуску оновлення.		
	Загальна оцінка реалізації вимоги 14.1			
14.2	Захист від шкідливого коду			
	A.14.2.ODP[01]	визначено частоту, з якою механізми захисту від шкідливого коду виконують перевірку;		
	A.14.2.1[01]	у визначених місцях системи впроваджено механізми захисту для виявлення шкідливого коду;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.14.2.1[02]	у визначених місцях системи впроваджено механізми захисту для знищення шкідливого коду;		
	A.14.2.2	механізми захисту від шкідливого коду оновлено з виходом нових версій відповідно до політики та процедур управління конфігурацією;		
	A.14.2.3.1[01]	механізми захисту від шкідливого коду налаштовано на виконання сканування системи <A.14.2.ODP[01]: частота>;		
	A.14.2.3.1[02]	механізми захисту від шкідливого коду налаштовано на виконання сканування файлів із зовнішніх джерел у режимі реального часу на кінцевих точках або точках входу та виходу з мережі під час завантаження, відкриття або виконання файлів;		
	A.14.2.3.2	механізми захисту від шкідливого коду налаштовано на блокування шкідливого коду, поміщення шкідливого коду в карантин або виконання інших дій у відповідь на виявлення шкідливого коду.		
	Загальна оцінка реалізації вимоги 14.2			
14.3	Попередження, рекомендації та директиви з безпеки			
	A.14.3.1	попередження, рекомендації та директиви щодо безпеки системи від зовнішніх організацій надходять на постійній основі;		
	A.14.3.2[01]	у разі потреби розробляються попередження, рекомендації та директиви щодо внутрішньої безпеки системи;		
	A.14.3.2[02]	у разі потреби розповсюджуються попередження, рекомендації та директиви щодо внутрішньої безпеки системи;		
	A.14.3.3	директиви з безпеки впроваджуються відповідно до встановлених часових рамок.		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	Загальна оцінка реалізації вимоги 14.3			
14.4	Моніторинг системи			
	A.14.4.1[01]	проводиться моніторинг системи з метою виявлення атак та індикаторів потенційних атак;		
	A.14.4.1[02]	проводиться моніторинг системи на предмет виявлення неавторизованих підключень;		
	A.14.4.2	виявляється несанкціоноване використання системи;		
	A.14.4.3[01]	проводиться моніторинг вхідного комунікаційного трафіка з метою виявлення незвичайних або несанкціонованих дій або умов;		
	A.14.4.3[02]	проводиться моніторинг вихідного комунікаційного трафіка з метою виявлення незвичайних або несанкціонованих дій або умов.		
	Загальна оцінка реалізації вимоги 14.4			
14.5	Управління та збереження інформації			
	A.14.05[01]	управління службовою інформацією в системі здійснюється відповідно до чинного законодавства, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог;		
	A.14.05[02]	збереження службової інформації в системі здійснюється відповідно до чинного законодавства, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог;		
	A.14.05[03]	виведення службової інформації з системи здійснюється відповідно до чинного законодавства, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.14.05[04]	виведена службова інформація з системи зберігається відповідно до чинного законодавства, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог.		
	Загальна оцінка реалізації вимоги 14.5			
15.1	Політика та процедури планування безпеки			
	A.15.1.1[01]	розроблені та задокументовані політики, необхідні для виконання вимог безпеки;		
	A.15.1.1[02]	політики, необхідні для виконання вимог безпеки, розповсюджуються серед персоналу або ролей організації;		
	A.15.1.1[03]	розроблені та задокументовані процедури, необхідні для виконання вимог безпеки;		
	A.15.1.1[04]	процедури, необхідні для виконання вимог безпеки, розповсюджуються серед персоналу або ролей організації;		
	A.15.1.2[01]	політики та процедури періодично переглядаються;		
	A.15.1.2[02]	політики та процедури періодично оновлюються.		
	Загальна оцінка реалізації вимоги 15.1			
15.2	Плани захисту інформації та персональних даних			
	A.15.2.1[01]	розроблено план захисту інформації, який визначає складові компоненти системи;		
	A.15.2.1[02]	розроблено план захисту інформації, який описує робоче середовище системи;		
	A.15.2.1[03]	розроблено план захисту інформації, який описує конкретні загрози системі, які викликають занепокоєння організації;		
	A.15.2.1[04]	розроблено план захисту інформації, який надає огляд вимог до безпеки системи;		
	A.15.2.1[05]	розроблено план захисту інформації, який визначає з'єднання з іншими системами;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.15.2.1[06]	розроблено план захисту інформації, який визначає осіб, що виконують ролі та обов'язки в системі;		
	A.15.2.1[07]	розроблено план захисту інформації, який містить іншу інформацію, необхідну для захисту службової інформації;		
	A.15.2.2[01]	план захисту інформації періодично переглядається;		
	A.15.2.2[02]	план захисту інформації періодично оновлюється;		
	A.15.2.3	план захисту інформації захищено від неавторизованого розголошення.		
	Загальна оцінка реалізації вимоги 15.2			
15.3	Правила поведінки			
	Мета оцінки визначити:		Оцінка висновок (позитивний/ негативний)	Коментарі та рекомендації експертів
	A.15.3.1[01]	створено правила, що описують обов'язки та очікувану поведінку при роботі зі службовою інформацією та використанням системи;		
	A.15.3.1[02]	правила поведінки щодо поводження зі службовою інформацією та використання системи надаються особам, яким потрібен доступ до системи;		
	A.15.3.2	отримується задокументоване підтвердження від фізичних осіб про те, що вони прочитали, зрозуміли та погодилися дотримуватися правил поведінки, отримані перед тим, як авторизувати доступ до службової інформації та системи;		
	A.15.3.3[01]	правила поведінки періодично переглядаються;		
	A.15.3.3[02]	правила поведінки періодично оновлюються.		
	Загальна оцінка реалізації вимоги 15.3			
16.1	Процес закупівель			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.16.1.ODP[01]	визначено вимоги до безпеки системи, компонента або послуги;		
	A.16.1	до договору про закупівлю системи, компонента системи або послуги вносяться наступні вимоги щодо безпеки: <A.16.01.ODP[01]: вимоги безпеки>.		
	Загальна оцінка реалізації вимоги 16.1			
16.2	Компоненти системи, що не підтримуються			
	A.16.2.1	компоненти системи замінюються, коли розробник, постачальник або виробник більше не надає підтримку цих компонентів;		
	A.16.2.2	у разі неможливості заміни компонентів, що не підтримуються, надаються варіанти зменшення ризиків або альтернативні джерела для продовження підтримки компонентів, що не підлягають заміні;		
	Загальна оцінка реалізації вимоги 16.2			
16.3	Компоненти системи, що не підтримуються			
	A.16.3.ODP[01]	визначено вимоги до безпеки, які мають застосовуватися зовнішніми постачальниками послуг для системи;		
	A.16.3.1	постачальники зовнішніх послуг для системи, що використовуються для обробки, зберігання або передачі службової інформації, дотримуються наступних вимог безпеки: <A.16.03.ODP[01]: вимоги безпеки>;		
	A.16.3.2	визначені та задокументовані ролі та обов'язки користувачів відносно зовнішніх послуг для системи, включаючи спільні обов'язки із зовнішніми постачальниками;		
	A.16.3.3	впроваджені процеси, методи та техніки для постійного моніторингу дотримання вимог безпеки зовнішніми постачальниками послуг.		
	Загальна оцінка реалізації вимоги 16.3			

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
17.1	План управління ризиками ланцюга постачання			
	A.17.1.1[01]	розроблено план управління ризиками ланцюга постачання;		
	A.17.1.1[02]	план управління ризиками ланцюга постачання враховує ризики, пов'язані з дослідженнями та розробкою системи, компонентів системи або послуг для системи;		
	A.17.1.1[03]	план управління ризиками ланцюга постачання враховує ризики, пов'язані з проектуванням системи, компонентів системи або послуг для системи;		
	A.17.1.1[04]	план управління ризиками ланцюга постачання враховує ризики, пов'язані з виробництвом системи, компонентів системи або послуг для системи;		
	A.17.1.1[05]	план управління ризиками ланцюга постачання враховує ризики, пов'язані з придбанням системи, компонентів системи або послуг для системи;		
	A.17.1.1[06]	план управління ризиками ланцюга постачання враховує ризики, пов'язані з постачанням системи, компонентів системи або послуг для системи;		
	A.17.1.1[07]	план управління ризиками ланцюга постачання охоплює ризики, пов'язані з інтеграцією системи, компонентів системи або послуг для системи;		
	A.17.1.1[08]	план управління ризиками ланцюга постачання охоплює ризики, пов'язані з експлуатацією та обслуговуванням системи, компонентів системи або служб в системі;		
	A.17.01.1[09]	план управління ризиками ланцюга постачання охоплює ризики, пов'язані з утилізацією системи, компонентів системи або служб в системі;		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
	A.17.1.2[01]	план управління ризиками ланцюга постачання періодично переглядається;		
	A.17.1.2[02]	план управління ризиками ланцюга постачання періодично оновлюється;		
	A.17.1.3	план управління ризиками ланцюга постачання захищений від несанкціонованого розголошення.		
	Загальна оцінка реалізації вимоги 17.1			
17.2	Стратегії придбання, інструменти і методи			
	A.17.2[01]	розроблено та впроваджено стратегії придбання, контрактні інструменти та методи придбання для виявлення ризиків у ланцюгу постачання;		
	A.17.2[02]	розроблено та впроваджено стратегії придбання, контрактні інструменти та методи придбання для захисту від ризиків ланцюга постачання;		
	A.17.2[03]	розроблено та впроваджено стратегії придбання, контрактні інструменти та методи придбання для зменшення ризиків у ланцюгу постачання.		
	Загальна оцінка реалізації вимоги 17.2			
17.3	Контроль ланцюга постачання і процесів			
	A.17.3.ODP[01]	визначені вимоги безпеки для захисту від ризиків ланцюга постачання для системи, компонентів системи або послуг для системи, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання;		
	A.17.3.1	запроваджено процес виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання;		
	A.17.3.2	наведені нижче вимоги безпеки застосовуються для захисту від ризиків ланцюга постачання для системи, компонентів системи або послуг для		

№ вимоги	Оцінка		Висновок з оцінки	Джерела отримання відомостей, коментарі оцінювача
	Позначення заходу з оцінки	Мета заходу з оцінки, визначити що:		
		системи, а також для обмеження шкоди або наслідків подій, пов'язаних з ланцюгом постачання: <A.17.3.ODP[01]: вимоги безпеки>.		
	Загальна оцінка реалізації вимоги 17.3			
Оцінка реалізації базового профілю				